9.3

Zabezpečení produktu IBM MQ

Poznámka

Než začnete používat tyto informace a produkt, který podporují, přečtěte si informace, které uvádí “Poznámky” na stránce 709.

Toto vydání se vztahuje na verzi 9 vydání 3 produktu IBM® MQ a na všechna následná vydání a úpravy, není-li v nových vydáních uvedeno jinak.

Obsah

zabezpečeníIBM MQ

Zabezpečení je důležitým aspektem jak pro vývojáře aplikací IBM MQ , tak pro administrátory systému IBM MQ . Jako naprosté minimum byste měli zajistit, aby veškerý hardware a software uvnitř zabezpečené zóny a na pracovních stanicích operátora byly v rámci životního cyklu podpory, aby byly aktuální s povinnými aktualizacemi softwaru a aby byly okamžitě použity aktualizace zabezpečení.

Související odkazy

IBM Správa ohrožení zabezpečení

z/OS Portál zabezpečení IBM Z a LinuxOne

přehled zabezpečení

Tato kolekce témat představuje koncepty zabezpečení IBM MQ .

Nejprve jsou představeny koncepce a mechanismy zabezpečení, které se vztahují k libovolnému počítačovému systému, a poté následuje diskuse o těchto mechanismech zabezpečení, které jsou implementovány v produktu IBM MQ.

Obecně uznávané aspekty bezpečnosti jsou následující:

- “Identifikace a autentizace” na stránce 7
- “Autorizace” na stránce 9
- “Auditování” na stránce 9
- “Důvěrnost” na stránce 9
- “Integrita dat” na stránce 10

Mechanizmy zabezpečení jsou technické nástroje a techniky, které se používají k implementaci služeb zabezpečení. Mechanizmus může fungovat sám nebo s ostatními, aby poskytoval určitou službu. Příklady běžných bezpečnostních mechanismů jsou následující:

- “Šifrování” na stránce 11
- “Výtahy zpráv a digitální podpisy” na stránce 12
- “digitální certifikáty” na stránce 13
- “infrastruktura veřejných klíčů (PKI)” na stránce 17

Při plánování implementace produktu IBM MQ zvažte, které mechanizmy zabezpečení potřebujete k implementaci těch aspektů zabezpečení, které jsou pro vás důležité. Informace o tom, co je třeba zvážit po přečtení těchto témat, viz “Plánování požadavků na zabezpečení” na stránce 85.

Identifikace a autentizace

Identifikace je schopnost jedinečně identifikovat uživatele systému nebo aplikace spuštěné v systému. *Ověření* je schopnost prokázat, že uživatel nebo aplikace je skutečně tím, za koho se tato osoba nebo jaká aplikace prohlašuje.

Zvažte například uživatele, který se přihlásí k systému zadáním ID uživatele a hesla. Systém používá ID uživatele k identifikaci uživatele. Systém ověří uživatele v době přihlášení tak, že zkontroluje, zda je zadané heslo správné.

Identifikace a ověření v produktu IBM MQ

Když se aplikace připojí k produktu IBM MQ, identita uživatele je vždy přidružena k připojení. Identita uživatele je na počátku ID uživatele operačního systému, které je přidruženo k procesu aplikace. Tato identita je často dostačující pro lokálně vázané aplikace, jejichž hostitelem je stejný systém jako správce front. Správce front však může také ověřit a upravit identitu přidruženou k připojení několika způsoby.

Ověřování identity přidružené k připojení je důležité v případě, že se klientské aplikace, které nemusí být nutně důvěryhodné, připojují ke správci front prostřednictvím sítě.

Identitu přidruženou k připojení aplikace ke správci front IBM MQ lze vytvořit pomocí některého z následujících mechanizmů:

- Když se aplikace připojí ke správci front, může poskytnout ID uživatele a heslo. Správce front ověřuje pověření na základě své konfigurace. Například ID uživatele a heslo lze předat operačnímu systému správce front nebo serveru LDAP k ověření.
- V 9.3.4 V produktu IBM MQ 9.3.4může aplikace také dodat token ověření, který získá z externího ověřovacího serveru. Další informace o tokenech ověření viz “Práce s tokeny ověření” na stránce 349.
- Kanál klienta lze konfigurovat pro použití vzájemného ověřování TLS, pokud je konfigurován s platným digitálním certifikátem. Ověření TLS lze kombinovat s pravidlem ověření kanálu (CHLAUTH), chcete-li k připojení přidružit odpovídající ID uživatele. Další informace viz “Jak TLS poskytuje identifikaci, ověření, důvěrnost a integritu” na stránce 20,
- Pravidla ověření kanálu (CHLAUTH) mohou přepsat identitu na základě informací o připojení. Pravidlo ověřování kanálu může například nastavit ID uživatele přidružené k připojení na základě adresy IP klienta.
- Vlastní kód ukončení může nastavit identitu na základě vámi zvolených kritérií.

Identita a ověřování jsou také použitelné pro kanály mezi dvěma správci front. Tyto kanály se nazývají kanály zpráv. Při spuštění kanálu zpráv může agent kanálu zpráv (MCA) na každém konci kanálu ověřit svého partnera. Tato technika se nazývá *vzájemné ověření*. Pro odesílající MCA poskytuje záruku, že partner, kterému se chystá odeslat zprávy, je skutečný. Podobně, přijímající MCA je zajištěno, že se chystá přijímat zprávy od skutečného partnera.

Po vytvoření identity, která je v případě potřeby ověřena, ji produkt IBM MQ používá několika způsoby:

- Důležité je, že při výchozím nastavení jsou všechny následné kontroly produktu “Autorizace” na stránce 9 prováděny s použitím této identity. Pokud se například aplikace pokusí vložit zprávu do fronty, správce front potvrdí, že identita přidružená k aplikaci má pro objekt fronty autorizaci 'put'.
- Kromě toho může každá zpráva obsahovat informace o *kontextu zprávy* . Tyto informace jsou uloženy v deskriptoru zpráv (MQMD). Správce front může automaticky generovat kontext zprávy, když aplikace vloží zprávu do fronty. Alternativně může aplikace dodat kontext zprávy, pokud je k tomu autorizováno ID uživatele přidružené k aplikaci. Tato kontextová informace ve zprávě poskytuje aplikaci, která přijímá informace o původci zprávy. Obsahuje například název aplikace, která vložila zprávu, a ID uživatele přidružené k aplikaci.

Neodmítání

Celkovým cílem nepopiratelné služby je dokázat, že určitá zpráva je spojena s konkrétní osobou.

Službu *non-repudiation* lze zobrazit jako rozšíření služby identifikace a ověření. Obecně platí, že nepopiratelnost se použije, když jsou údaje přenášeny elektronicky; například příkaz k nákupu nebo prodeji akcií burzovním makléřem nebo příkaz k bankovnímu převodu prostředků z jednoho účtu na druhý.

Služba neodmítání může obsahovat více než jednu komponentu, kde každá komponenta poskytuje jinou funkci. Pokud odesílatel zprávy někdy odmítne odeslání zprávy, může služba neodmítání s *dokladem o původu* poskytnout příjemci nepopiratelný důkaz o tom, že zpráva byla odeslána konkrétní osobou. Pokud příjemce zprávy někdy popírá její přijetí, může nepopiratelná služba s *dokladem o doručení* poskytnout odesílateli nepopiratelný důkaz o tom, že zpráva byla přijata konkrétní osobou.

V praxi je důkaz s téměř 100% jistotou, nebo nepopiratelný důkaz, obtížným cílem. V reálném světě není nic zcela bezpečné. Správa zabezpečení se více zabývá správou rizik na úrovni, která je pro podnik přijatelná. V takovém prostředí, realističtější očekávání non-repudiation služby je být schopen poskytnout důkazy, které jsou přípustné, a podporuje váš případ, u soudu.

Nepopiratelnost je relevantní bezpečnostní služba v IBM MQ prostředí, protože IBM MQ je prostředkem elektronického přenosu dat. Můžete například požadovat současný důkaz o tom, že konkrétní zpráva byla odeslána nebo přijata aplikací přidruženou k určité osobě.

IBM MQ with Advanced Message Security neposkytuje službu neodmítání jako součást své základní funkce. Tato dokumentace k produktu však obsahuje návrhy, jak můžete poskytnout svou vlastní službu neodmítání v rámci prostředí IBM MQ tím, že napíšete své vlastní uživatelské programy.

Autorizace

Autorizace chrání kritické prostředky v systému tím, že omezuje přístup pouze na autorizované uživatele a jejich aplikace. Zabraňuje neoprávněnému použití prostředku nebo použití prostředku neautorizovaným způsobem.

Autorizace v souboru IBM MQ

Můžete použít autorizaci k omezení toho, co mohou konkrétní jednotlivci nebo aplikace provádět ve vašem prostředí IBM MQ .

Zde je několik příkladů autorizace v prostředí IBM MQ :

- Povolení pouze autorizovanému administrátorovi vydávat příkazy pro správu prostředků IBM MQ .
- Povolení připojení aplikace ke správci front pouze v případě, že je k tomu autorizováno jméno uživatele přidružené k aplikaci.
- Povolení aplikaci otevřít pouze ty fronty, které jsou nezbytné pro její funkci.
- Povolení, aby se aplikace přihlásili pouze k odběru témat, která jsou nezbytná pro její funkci.
- Umožňuje aplikaci provádět pouze ty operace ve frontě, které jsou nezbytné pro její funkci. Aplikace může například potřebovat pouze procházet zprávy v konkrétní frontě a nevkládat ani nezískávat zprávy.

Další informace o nastavení autorizace viz téma "Autorizace plánování" na stránce 88 a přidružená dílčí témata.

Auditování

Auditování je proces zaznamenávání a kontroly událostí za účelem zjištění, zda došlo k neočekávané nebo neoprávněné aktivitě nebo zda došlo k pokusu o provedení takové aktivity.

Auditování v adresáři IBM MQ

Produkt IBM MQ může vydávat zprávy událostí, které zaznamenávají, že došlo k neobvyklé aktivitě.

Zde je několik příkladů auditování v prostředí IBM MQ :

- Aplikace se pokusí otevřít frontu, pro kterou nemá oprávnění k otevření. Je vydána zpráva události instrumentace. Kontrolou zprávy události zjistíte, že k tomuto pokusu došlo, a můžete se rozhodnout, jaká akce je nezbytná.
- Aplikace se pokusí otevřít kanál, ale pokus se nezdaří, protože připojení TLS není povoleno. Je vydána zpráva události instrumentace. Kontrolou zprávy události zjistíte, že k tomuto pokusu došlo, a můžete se rozhodnout, jaká akce je nezbytná.

Důvěrnost

Služba *důvěrnost* chrání citlivé informace před neoprávněným zveřejněním.

Když jsou citlivá data uložena lokálně, mechanizmy řízení přístupu mohou být dostatečné k jejich ochraně za předpokladu, že data nelze přečíst, pokud k nim nelze přistupovat. Je-li vyžadována vyšší úroveň zabezpečení, lze data šifrovat.

Šifrovat citlivá data, když jsou přenášena přes komunikační síť, zejména přes nezabezpečenou síť, jako je Internet. V síťovém prostředí nejsou mechanismy řízení přístupu účinné proti pokusům o zachycení dat, například odposlechu.

Důvěrnost v IBM MQ

V produktu IBM MQ můžete implementovat utajení šifrováním zpráv.

V prostředí IBM MQ lze zajistit důvěrnost následujícím způsobem:

- Poté, co odesílající agent MCA obdrží zprávu z přenosové fronty, produkt IBM MQ použije protokol TLS k zašifrování zprávy před jejím odesláním přes síť přijímajícímu agentovi MCA. Na druhém konci kanálu je zpráva dešifrována před tím, než ji přijímající agent MCA vloží do své cílové fronty.
- Zatímco jsou zprávy uloženy v lokální frontě, mechanizmy řízení přístupu poskytované produktem IBM MQ mohou být považovány za dostatečné pro ochranu jejich obsahu před neoprávněným zveřejněním. Pro vyšší úroveň zabezpečení však můžete použít produkt Advanced Message Security k šifrování zpráv uložených ve frontách.
- z/OS Zprávy uložené v lokálních frontách lze šifrovat v klidu pomocí šifrování datové sady z/OS .

  Viz část důvěrnost pro data v klidu na systému IBM MQ for z/OS se šifrováním datové sady. Další informace viz.

Integrita dat

Služba *integrity dat* zjišťuje, zda došlo k neoprávněným úpravám dat.

Existují dva způsoby, jak mohou být data pozměněna: náhodně, prostřednictvím hardwarových a přenosových chyb, nebo kvůli úmyslnému útoku. Mnoho hardwarových produktů a přenosových protokolů má mechanismy pro detekci a opravu hardwarových a přenosových chyb. Účelem služby integrity dat je zjistit úmyslný útok.

Cílem služby integrity dat je pouze zjistit, zda byla data upravena. Neusiluje o obnovení dat do původního stavu, pokud byla upravena.

Mechanismy řízení přístupu mohou přispět k integritě dat, pokud data nelze změnit, pokud je přístup odepřen. Stejně jako v případě důvěrnosti však nejsou mechanismy kontroly přístupu v síťovém prostředí účinné.

Integrita dat v produktu IBM MQ

Integritu dat lze zajistit v prostředí IBM MQ takto:

- Pomocí protokolu TLS můžete zjistit, zda byl obsah zprávy během přenosu po síti záměrně upraven. V protokolu TLS poskytuje algoritmus výběru zpráv detekci změněných zpráv při přenosu.

  Všechny specifikace IBM MQ CipherSpecs poskytují algoritmus kódu digest zprávy, s výjimkou algoritmu TLS_RSA_WITH_NULL_NULL, který neposkytuje integritu dat zprávy.

  Produkt IBM MQ zjišťuje upravené zprávy po jejich přijetí; při přijetí upravené zprávy IBM MQ se do protokolu chyb zapíše chybová zpráva AMQ9661 a kanál se zastaví.
- Zatímco jsou zprávy uloženy v lokální frontě, mechanizmy řízení přístupu poskytované produktem IBM MQ mohou být považovány za dostatečné, aby zabránily záměrným úpravám obsahu zpráv.

  Pro vyšší úroveň zabezpečení však můžete použít produkt Advanced Message Security ke zjištění, zda byl obsah zprávy záměrně upraven mezi okamžikem, kdy byla zpráva vložena do fronty, a okamžikem, kdy byla načtena z fronty.

  Pokud je zjištěna upravená zpráva, aplikace, která se pokouší přijmout zprávu, obdrží návratový kód MQRC_SECURITY_ERROR (2063). Pokud aplikace používá volání MQGET , zpráva se také přesune do SYSTEM.PROTECTION.ERROR.QUEUE .

Kryptografické koncepty

Tato kolekce témat popisuje koncepty šifrování použitelné pro produkt IBM MQ.

Termín *entita* se používá k odkazování na správce front, IBM MQ MQI client, jednotlivého uživatele nebo jakýkoli jiný systém schopný výměny zpráv.

Šifrování

Šifrování je proces převodu mezi čitelným textem, který se nazývá *prostý text*, a nečitelnou formou, která se nazývá *šifrovaný text*.

K tomu dochází takto:

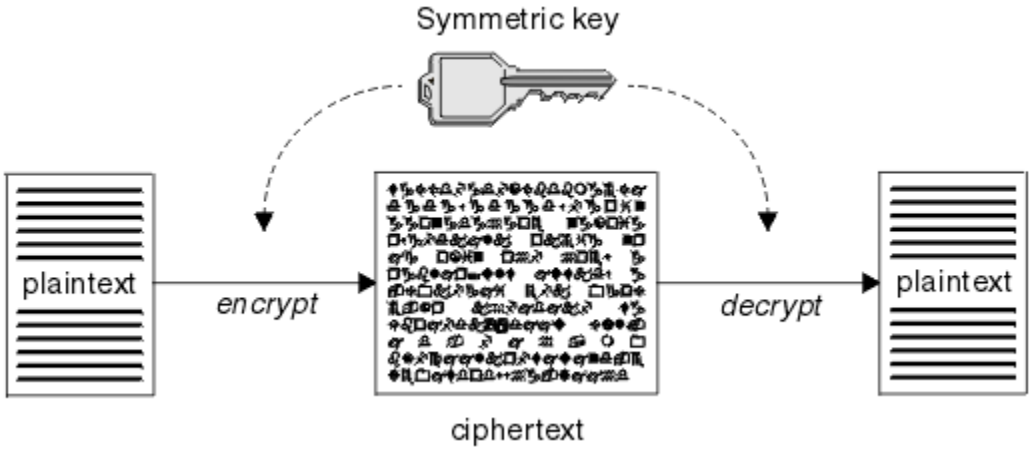
1. Odesílatel převede zprávu ve formátu prostého textu na šifrovaný text. Tato část procesu se nazývá *šifrování* (někdy *šifrování*).
2. Šifrovaný text je přenesen do přijímače.
3. Přijímač převádí zprávu šifrovaného textu zpět do formátu prostého textu. Tato část procesu se nazývá *dešifrování* (někdy *dešifrování*).

Převod zahrnuje posloupnost matematických operací, které mění vzhled zprávy během přenosu, ale neovlivňují obsah. Kryptografické techniky mohou zajistit důvěrnost a chránit zprávy před neoprávněným zobrazením (odposlouchávání), protože šifrovaná zpráva není pochopitelná. Digitální podpisy, které poskytují záruku integrity zpráv, používají šifrovací techniky. Další informace viz “Digitální podpisy v SSL/TLS” na stránce 22.

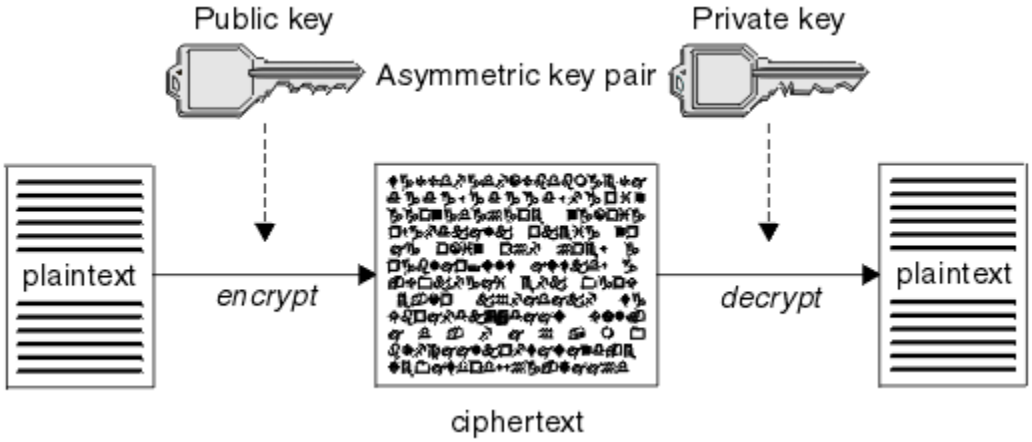
Kryptografické techniky zahrnují obecný algoritmus, který je specifický pro použití klíčů. Existují dvě třídy algoritmu:

- Ty, které vyžadují, aby obě strany používaly stejný tajný klíč. Algoritmy, které používají sdílený klíč, se nazývají *symetrické* algoritmy. Obrázek 1 na stránce 11 ilustruje šifrování symetrického klíče.
- Ty, které používají jeden klíč pro šifrování a jiný klíč pro dešifrování. Jeden z nich musí být tajný, ale druhý může být veřejný. Algoritmy, které používají dvojice veřejných a soukromých klíčů, se nazývají *asymetrické* algoritmy. Obrázek 2 na stránce 12 ilustruje šifrování s asymetrickým klíčem, které je také známé jako *šifrování s veřejným klíčem*.

Použité šifrovací a dešifrovací algoritmy mohou být veřejné, ale sdílený tajný klíč a soukromý klíč musí být tajný.



Obrázek 1. šifrování pomocí symetrických klíčů



Obrázek 2. šifrování pomocí asymetrických klíčů

Obrázek 2 na stránce 12 ukazuje prostý text zašifrovaný veřejným klíčem příjemce a dešifrovaný soukromým klíčem příjemce. Pouze zamýšlený zásobník uchovává soukromý klíč pro dešifrování šifrovaného textu. Všimněte si, že odesílatel může také šifrovat zprávy pomocí soukromého klíče, což umožňuje komukoli, kdo drží veřejný klíč odesílatele, dešifrovat zprávu s jistotou, že zpráva musí pocházet od odesílatele.

Pomocí asymetrických algoritmů jsou zprávy šifrovány buď veřejným, nebo soukromým klíčem, ale lze je dešifrovat pouze s jiným klíčem. Pouze soukromý klíč je tajný, veřejný klíč může být znám kýmkoli. U symetrických algoritmů musí být sdílený klíč znám pouze oběma stranám. Tomu se říká *problém s distribucí klíčů*. Asymetrické algoritmy jsou pomalejší, ale mají tu výhodu, že neexistuje žádný problém s distribucí klíčů.

Další terminologie spojená s kryptografií je:

Síla
Síla šifrování je určena velikostí klíče. Asymetrické algoritmy vyžadují velké klíče, například:

1024 bitů	Asymetrický klíč s nízkou pevností
2048 bitů	Asymetrický klíč střední síly
4096 bitů	Asymetrický klíč s vysokou pevností

Symetrické klíče jsou menší: 256 bitové klíče poskytují silné šifrování.

Algoritmus blokové šifry
Tyto algoritmy šifrují data podle bloků. Například algoritmus RC2 z RSA Data Security Inc. používá bloky dlouhé 8 bajtů. Blokové algoritmy jsou obvykle pomalejší než proudové algoritmy.

Algoritmus šifrování proudu
Tyto algoritmy pracují na každém bajtu dat. Proudové algoritmy jsou obvykle rychlejší než blokové algoritmy.

Výtahy zpráv a digitální podpisy

Kód digest zprávy je číselná reprezentace obsahu zprávy s pevnou velikostí. Kód digest zprávy je vypočítán pomocí hašovací funkce a lze jej zašifrovat a vytvořit tak digitální podpis.

Hašovací funkce použitá k výpočtu kódu digest zprávy musí splňovat dvě kritéria:

- Musí to být jednosměrné. Nesmí být možné zvrátit funkci pro vyhledání zprávy odpovídající určitému kódu digest zprávy, jinak než testováním všech možných zpráv.
- Musí být výpočetně neproveditelné najít dvě zprávy, které hašují na stejný kód digest.

Kód digest zprávy je odeslán se samotnou zprávou. Příjemce může vygenerovat kód digest pro zprávu a porovnat jej s algoritmem digest odesilatele. Integrita zprávy je ověřena, když jsou dva výtahy zprávy stejné. Jakákoli manipulace se zprávou během přenosu téměř jistě vede k jinému kódu digest zprávy.

Kód digest zprávy vytvořený pomocí tajného symetrického klíče je znám jako kód MAC (Message Authentication Code), protože může poskytnout jistotu, že zpráva nebyla upravena.

Odesílatel může také vygenerovat kód digest zprávy a poté kód digest zašifrovat pomocí soukromého klíče páru asymetrických klíčů, který vytvoří digitální podpis. Podpis pak musí být dešifrován příjemcem, než jej porovnáte s lokálně generovaným digestem.

Související pojmy

“Digitální podpisy v SSL/TLS” na stránce 22
Digitální podpis je tvořen šifrováním reprezentace zprávy. Šifrování používá soukromý klíč signatáře a z důvodu efektivity obvykle pracuje na kódu digest zprávy, nikoli na zprávě samotné.

digitální certifikáty

Digitální certifikáty chrání před zosobněním, což potvrzuje, že veřejný klíč patří určené entitě. Jsou vydávány certifikační autoritou.

Digitální certifikáty poskytují ochranu před zosobněním, protože digitální certifikát váže veřejný klíč k vlastníkovi, ať už je tento vlastník jednotlivec, správce front nebo jiná entita. Digitální certifikáty jsou také známé jako certifikáty veřejného klíče, protože vám poskytují záruky o vlastnictví veřejného klíče, když používáte schéma asymetrického klíče. Digitální certifikát obsahuje veřejný klíč pro entitu a je prohlášením, že veřejný klíč patří této entitě:

- Je-li certifikát určen pro jednotlivou entitu, nazývá se *osobní certifikát* nebo *uživatelský certifikát*.
- Je-li certifikát určen pro certifikační autoritu, nazývá se certifikát *certifikátem certifikační autority* nebo *certifikátem podepsaného*.

Pokud jsou veřejné klíče odesílány přímo jejich vlastníkem jiné entitě, existuje riziko, že by mohla být zpráva zachycena a veřejný klíč nahrazen jiným. Toto je známé jako *muž ve středním útoku*. Řešením tohoto problému je výměna veřejných klíčů prostřednictvím důvěryhodné třetí strany, což vám dává silnou záruku, že veřejný klíč skutečně patří k subjektu, se kterým komunikujete. Místo toho, abyste veřejný klíč odeslali přímo, požádejte důvěryhodnou třetí stranu, aby jej začlenila do digitálního certifikátu. Důvěryhodná třetí strana, která vydává digitální certifikáty, se nazývá certifikační autorita (CA), jak je popsáno v tématu “Certifikační autority” na stránce 14.

Co je v digitálním certifikátu

Digitální certifikáty obsahují specifické informace určené standardem X.509 .

Digitální certifikáty používané produktem IBM MQ jsou v souladu se standardem X.509 , který určuje požadované informace a formát pro jejich odeslání. X.509 je část rámce ověřování řady standardů X.500 .

Digitální certifikáty obsahují alespoň tyto informace o certifikovaném subjektu:

- Veřejný klíč vlastníka
- Rozlišující název vlastníka
- Rozlišující název certifikační autority, která vydala certifikát
- Datum, od kterého je certifikát platný
- Datum ukončení platnosti osvědčení
- Číslo verze datového formátu certifikátu, jak je definováno v X.509. Aktuální verze standardu X.509 je verze 3 a většina certifikátů odpovídá této verzi.
- Sériové číslo. Jedná se o jedinečný identifikátor přiřazený certifikační autoritou, která vydala certifikát. Sériové číslo je jedinečné v rámci certifikační autority, která vydala certifikát: žádné dva certifikáty podepsané stejným certifikátem certifikační autority nemají stejné sériové číslo.

Certifikát X.509 verze 2 také obsahuje identifikátor vydavatele a identifikátor subjektu a certifikát X.509 verze 3 může obsahovat řadu rozšíření. Některá rozšíření certifikátu, například rozšíření Základní omezení,

jsou *standardní*, ale jiná jsou specifická pro implementaci. Rozšíření může být *kritické*, v takovém případě musí být systém schopen rozpoznat pole; pokud nerozpozná pole, musí odmítnout certifikát. Není-li přípona kritická, může ji systém ignorovat, pokud ji nerozpozná.

Digitální podpis v osobním certifikátu je generován pomocí soukromého klíče certifikační autority, která tento certifikát podepsala. Každý, kdo potřebuje ověřit osobní certifikát, k tomu může použít veřejný klíč CA. Certifikát CA obsahuje svůj veřejný klíč.

Digitální certifikáty neobsahují váš soukromý klíč. Musíš držet svůj soukromý klíč v tajnosti.

Požadavky na osobní certifikáty

Produkt IBM MQ podporuje digitální certifikáty, které jsou v souladu se standardem X.509 . Vyžaduje volbu ověření klienta.

Vzhledem k tomu, že IBM MQ je systém typu peer-to-peer, je v terminologii SSL/TLS považován za ověření klienta. Proto musí každý osobní certifikát použitý pro ověření SSL/TLS povolit použití klíče pro ověření klienta. Ne všechny certifikáty serveru mají tuto volbu povolenou, takže poskytovatel certifikátů možná bude muset povolit ověření klienta v kořenové certifikační autoritě pro zabezpečený certifikát.

Kromě standardů, které specifikují formát dat pro digitální certifikát, existují také normy pro určení, zda je certifikát platný. Tyto standardy byly v průběhu času aktualizovány, aby se zabránilo určitým typům narušení bezpečnosti. Například starší certifikáty X.509 verze 1 a 2 neoznačovaly, zda lze certifikát legitimně použít k podepisování jiných certifikátů. Proto bylo možné, aby uživatel se zlými úmysly získal osobní certifikát z legitimního zdroje a vytvořil nové certifikáty určené k zosobnění jiných uživatelů.

Při použití certifikátů X.509 verze 3 se rozšíření certifikátu BasicConstraints a KeyUsage používají k určení, které certifikáty mohou legitimně podepisovat jiné certifikáty. Standard IETF RFC 5280 specifikuje řadu pravidel pro ověření platnosti certifikátu, která musí být v souladu s aplikačním softwarem implementována, aby se zabránilo útokům na zosobnění. Sada pravidel certifikátu je známá jako zásada ověření platnosti certifikátu.

Další informace o zásadách ověřování certifikátů v tématu IBM MQnaleznete v části “Zásady ověřování certifikátů v adresáři IBM MQ” na stránce 44.

Certifikační autority

Certifikační autorita (CA) je důvěryhodná třetí strana, která vydává digitální certifikáty, aby vám poskytla záruku, že veřejný klíč entity skutečně patří k této entitě.

Role certifikační autority jsou:

- Po obdržení žádosti o digitální certifikát ověřit identitu žadatele před sestavením, podpisem a vrácením osobního certifikátu.
- Poskytnutí vlastního veřejného klíče CA v jeho certifikátu CA
- Chcete-li publikovat seznamy certifikátů, které již nejsou důvěryhodné v seznamu odvolaných certifikátů (CRL). Další informace viz “Práce se zrušenými certifikáty” na stránce 359
- Poskytnutí přístupu ke stavu odvolání certifikátu provozováním serveru odpovídacího modulu OCSP.

Rozlišující názvy

Rozlišující název (DN) jedinečně identifikuje entitu v certifikátu X.509 .

Upozornění: Ve filtru SSLPEER lze použít pouze atributy v následující tabulce. DN certifikátů mohou obsahovat jiné atributy, ale filtrování není u těchto atributů povoleno.

Tabulka 1. Typy atributů nalezené v DN, které lze použít ve filtru SSLPEER

Typ atributu	**Popis**
SERIALNUMBER	Sériové číslo certifikátu
MAIL	E-mailová adresa
Deprecated E	E-mailová adresa (zamítnuto ve prospěch volby MAIL)

Tabulka 1. Typy atributů nalezené v DN, které lze použít ve filtru SSLPEER (pokračování)	
Typ atributu	**Popis**
UID nebo USERID	Identifikátor uživatele
CN	Obecný název
T	Titulek
OU	Název organizační jednotky
DC	Komponenta domény
O	Název organizace
STREET	Ulice/první řádek adresy
L	Název umístění
ST (nebo SP či S)	Název státu nebo správního celku
Osobní počítač	PSČ
C	Země
UNSTRUCTUREDNAME	Název hostitele
UNSTRUCTUREDADDRESS	Adresa IP
DNQ	Kvalifikátor rozlišujícího názvu

Standard X.509 definuje další atributy, které obvykle netvoří část DN, ale mohou poskytovat volitelná rozšíření digitálního certifikátu.

Standard X.509 poskytuje DN, které má být uvedeno ve formátu řetězce. Příklad:

```
CN=John Smith, OU=Test, O=IBM, C=GB
```

Obecný název (CN) může popisovat jednotlivého uživatele nebo jakoukoli jinou entitu, například webový server.

DN může obsahovat více atributů OU a DC. Je povolena pouze jedna instance každého z ostatních atributů. Pořadí položek organizační jednotky je významné: pořadí uvádí hierarchii názvů organizačních jednotek, s jednotkou nejvyšší úrovně jako první. Pořadí položek DC je také významné.

IBM MQ toleruje určitá chybná DN. Další informace viz IBM MQ pravidla pro hodnoty SSLPEER.

Související pojmy

“Co je v digitálním certifikátu” na stránce 13

Digitální certifikáty obsahují specifické informace určené standardem X.509 .

Získání osobních certifikátů od certifikační autority

Certifikát můžete získat od důvěryhodné externí certifikační autority (CA).

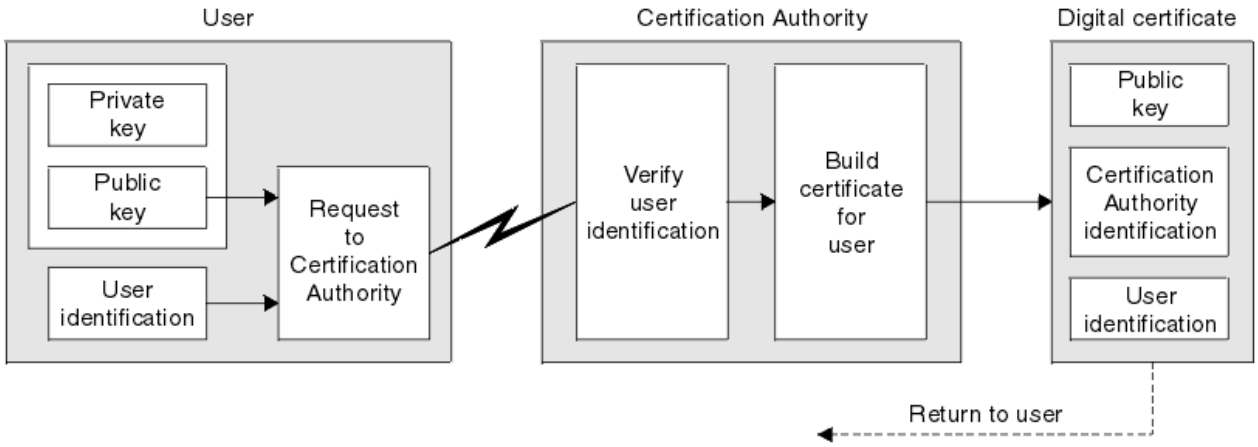
Digitální certifikát získáte odesláním informací certifikační autoritě ve formě žádosti o certifikát. Standard X.509 definuje formát pro tyto informace, ale některé certifikační autority mají svůj vlastní formát. Požadavky na certifikáty jsou obvykle generovány nástrojem pro správu certifikátů, který váš systém používá; například:

- Multi Příkaz **strmqikm** (nástrojiKeyman) na systému Multiplatformsa příkazy **runmqckm** a **runmqakm** na systému AIX, Linux, and Windows.
- z/OS RACF zapnuto z/OS.

Informace obsahují vaše rozlišovací jméno a váš veřejný klíč. Když váš nástroj pro správu certifikátů vygeneruje váš požadavek na certifikát, vygeneruje také váš soukromý klíč, který musíte udržovat v bezpečí. Nikdy nedistribuujte svůj soukromý klíč.

Jakmile certifikační autorita obdrží vaši žádost, ověří vaši identitu před sestavením certifikátu a vrátí vám jej jako osobní certifikát.

Obrázek 3 na stránce 16 ilustruje proces získání digitálního certifikátu od CA.



Obrázek 3. Získání digitálního certifikátu

V diagramu:

- Identifikace uživatele zahrnuje vaše rozlišovací jméno subjektu.
- Identifikace certifikační autority zahrnuje rozlišující název certifikační autority, která vydává certifikát.

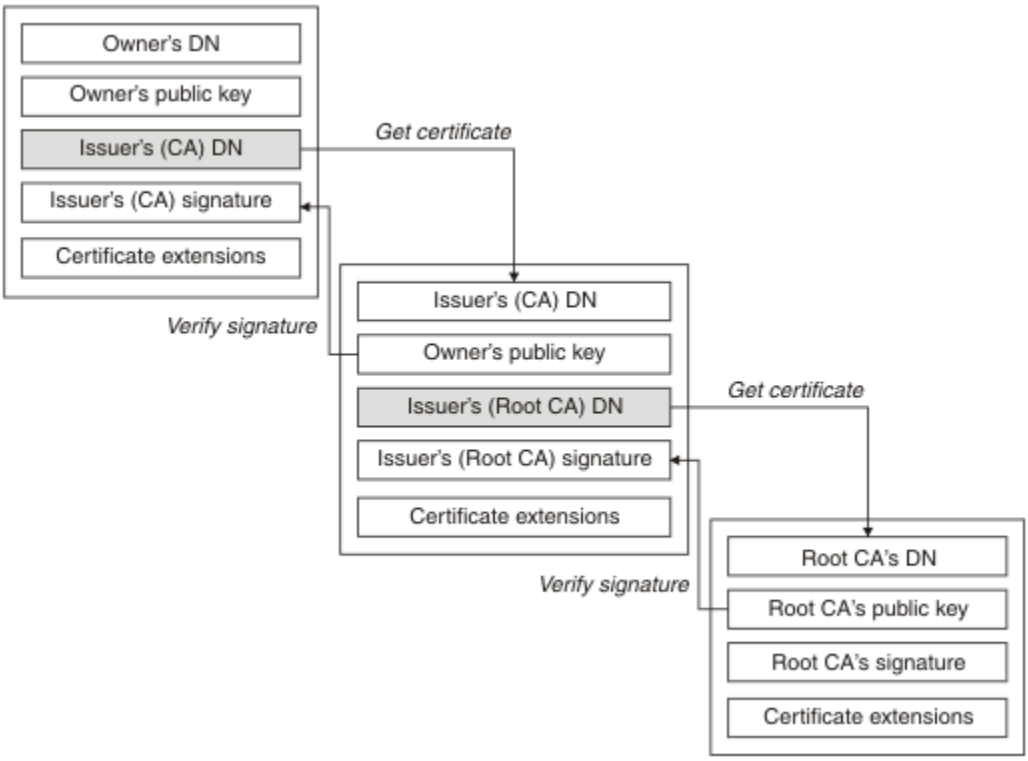
Digitální certifikáty obsahují další pole jiná než ta, která jsou uvedena v diagramu. Další informace o ostatních polích v digitálním certifikátu viz “Co je v digitálním certifikátu” na stránce 13.

Jak fungují řetězy certifikátů

Když obdržíte certifikát pro jinou entitu, možná budete muset použít *řetěz certifikátů* , abyste získali certifikát *kořenové CA* .

Řetěz certifikátů, známý také jako *certifikační cesta*, je seznam certifikátů použitých k ověření entity. Řetězec nebo cesta začíná certifikátem této entity a každý certifikát v řetězci je podepsán entitou identifikovanou dalším certifikátem v řetězci. Řetěz se ukončí s kořenovým certifikátem CA. Kořenový certifikát CA je vždy podepsán samotnou certifikační autoritou (CA). Podpisy všech certifikátů v řetězci musí být ověřeny, dokud není dosaženo kořenového certifikátu CA.

Obrázek 4 na stránce 17 znázorňuje cestu certifikace od vlastníka certifikátu ke kořenové certifikační autoritě, kde začíná řetězec důvěryhodnosti.



Obrázek 4. Řetězec důvěry

Každý certifikát může obsahovat jednu nebo více přípon. Certifikát náležející certifikační autoritě obvykle obsahuje rozšíření BasicConstraints s nastaveným příznakem isCA , který označuje, že je povoleno podepisovat jiné certifikáty.

Když již certifikáty nejsou platné

Digitální certifikáty mohou vypršet nebo mohou být odvolány.

Digitální certifikáty jsou vydávány na dobu určitou a nejsou platné po uplynutí doby platnosti.

Certifikáty mohou být odvolány z různých důvodů, včetně:

- Vlastník se přesunul do jiné organizace.
- Soukromý klíč již není tajný.

Produkt IBM MQ může zkontrolovat, zda je certifikát odvolán, odesláním požadavku odpovídacímu modulu OCSP (Online Certificate Status Protocol) (pouze na systému AIX, Linux, and Windows). Případně mohou přistupovat k seznamu odvolaných certifikátů (CRL) na serveru LDAP. Informace o odvolání protokolu OCSP a CRL jsou publikovány certifikační autoritou. Další informace viz “Práce se zrušenými certifikáty” na stránce 359.

infrastruktura veřejných klíčů (PKI)

Infrastruktura PKI (Public Key Infrastructure) je systém zařízení, zásad a služeb, který podporuje použití šifrování pomocí veřejného klíče pro ověření stran zapojených do transakce.

Neexistuje jediný standard, který by definoval komponenty infrastruktury veřejných klíčů, ale infrastruktura PKI se obvykle skládá z certifikačních autorit (CA) a registračních autorit (RAs). Certifikační autority poskytují následující služby:

- Vydávání digitálních certifikátů
- Ověření digitálních certifikátů
- Odvolání digitálních certifikátů

- Distribuce veřejných klíčů

Standardy X.509 poskytují základ pro průmyslový standard Public Key Infrastructure.

Další informace o digitálních certifikátech a certifikačních autoritách (CA) naleznete v části “digitální certifikáty” na stránce 13 . RA ověří informace poskytnuté při vyžádání digitálních certifikátů. Pokud RA tyto informace ověří, může certifikační autorita vydat žadateli digitální certifikát.

Infrastruktura PKI může také poskytovat nástroje pro správu digitálních certifikátů a veřejných klíčů. Infrastruktura PKI je někdy popsána jako *hierarchie důvěryhodnosti* pro správu digitálních certifikátů, ale většina definic zahrnuje další služby. Některé definice zahrnují služby šifrování a digitálního podpisu, ale tyto služby nejsou nezbytné pro provoz infrastruktury PKI.

Šifrovací bezpečnostní protokoly: TLS

Šifrovací protokoly poskytují zabezpečená připojení, což umožňuje dvěma stranám komunikovat se soukromím a integritou dat. Protokol TLS (Transport Layer Security) se vyvinul z protokolu SSL (Secure Sockets Layer). Produkt IBM MQ podporuje protokol TLS.

Primárním cílem obou protokolů je zajistit důvěrnost (někdy označovaná jako *soukromí*), integritu dat, identifikaci a ověření pomocí digitálních certifikátů.

Ačkoli jsou oba protokoly podobné, rozdíly jsou natolik významné, že SSL 3.0 a různé verze TLS nespolupracují.

Související pojmy

“Protokoly zabezpečení TLS v adresáři IBM MQ” na stránce 24
Produkt IBM MQ podporuje protokol TLS (Transport Layer Security), který poskytuje zabezpečení na úrovni propojení pro kanály zpráv a kanály MQI.

Koncepce TLS (Transport Layer Security)

Protokol TLS umožňuje dvěma stranám vzájemně se identifikovat a ověřovat a komunikovat s důvěrností a integritou dat. Protokol TLS se vyvinul z protokolu Netscape SSL 3.0 , ale protokoly TLS a SSL nespolupracují.

Protokol TLS poskytuje zabezpečení komunikace přes internet a umožňuje aplikacím typu klient/server komunikovat způsobem, který je důvěrný a spolehlivý. Protokoly mají dvě vrstvy: Record Protocol a Handshake Protocol, a ty jsou vrstvené nad přenosovým protokolem, například TCP/IP. Oba používají asymetrické a symetrické kryptografické techniky.

Připojení TLS je zahájeno aplikací, která se stane klientem TLS. Aplikace, která přijme připojení, se stane serverem TLS. Každá nová relace začíná handshake, jak je definováno protokoly TLS.

Úplný seznam specifikací CipherSpecs podporovaných produktem IBM MQ je k dispozici na adrese “Povolení CipherSpecs” na stránce 438.

Další informace o protokolu SSL naleznete v informacích uvedených na adrese https://developer.mozilla.org/docs/Mozilla/Projects/NSS. Další informace o protokolu TLS naleznete v informacích poskytnutých pracovní skupinou TLS na webu skupiny Internet Engineering Task Force na adrese https://www.ietf.org

Přehled navázání komunikace SSL/TLS

Navázání komunikace SSL/TLS umožňuje klientovi a serveru TLS zavést tajné klíče, se kterými komunikují.

Tento oddíl poskytuje souhrn kroků, které umožňují vzájemnou komunikaci klienta a serveru TLS.

- Dohodnout se na verzi protokolu, který má být použit.
- Vyberte šifrovací algoritmy.
- Vzájemně se ověřovat výměnou a ověřením digitálních certifikátů.

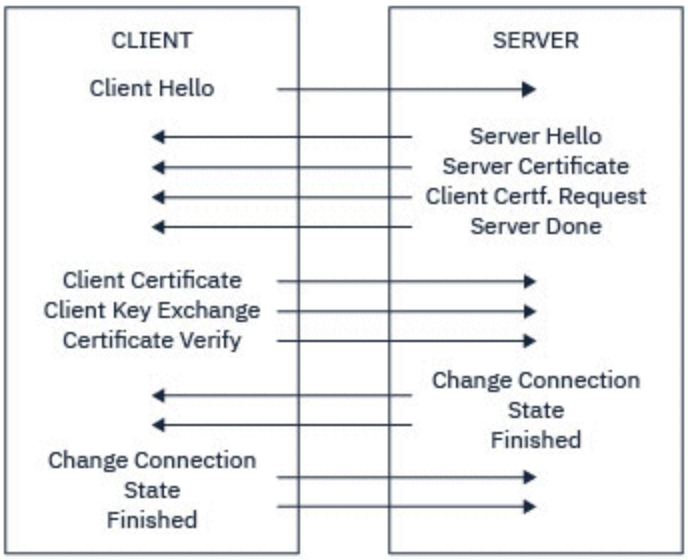
- Pomocí asymetrických technik šifrování vygenerujte sdílený tajný klíč, čímž se vyhnete problému s distribucí klíčů. TLS pak použije sdílený klíč pro symetrické šifrování zpráv, což je rychlejší než asymetrické šifrování.

Další informace o šifrovacích algoritmech a digitálních certifikátech naleznete v souvisejících informacích.

V přehledu jsou do navázání komunikace TLS zahrnuty následující kroky:

1. Klient TLS odešle zprávu "hello klienta" , která vypíše kryptografické informace, jako např. verzi TLS, a v upřednostňovaném pořadí klienta CipherSuites podporované klientem. Zpráva také obsahuje náhodný bajtový řetězec, který se používá v následných výpočtech. Protokol umožňuje "klientskému modulu hello" zahrnout metody komprese dat podporované klientem.
2. Server TLS odpovídá zprávou "server ahoj" , která obsahuje sadu CipherSuite zvolenou serverem ze seznamu poskytnutého klientem, ID relace a jiný náhodný bajtový řetězec. Server také odesílá svůj digitální certifikát. Pokud server vyžaduje digitální certifikát pro ověření klienta, odešle "žádost o certifikát klienta" , která obsahuje seznam typů podporovaných certifikátů a rozlišující názvy přijatelných certifikačních autorit (CA).
3. Klient TLS ověří digitální certifikát serveru. Další informace viz téma “Jak TLS poskytuje identifikaci, ověření, důvěrnost a integritu” na stránce 20.
4. Klient TLS odešle náhodný bajtový řetězec, který umožní klientovi i serveru vypočítat tajný klíč, který se má použít pro šifrování následných dat zprávy. Samotný náhodný bajtový řetězec je šifrován pomocí veřejného klíče serveru.
5. Pokud server TLS odeslal "žádost o certifikát klienta", odešle klient náhodný bajtový řetězec zašifrovaný soukromým klíčem klienta spolu s digitálním certifikátem klienta nebo "bez výstrahy digitálního certifikátu". Tato výstraha je pouze varováním, ale s některými implementacemi se navázání komunikace nezdaří, pokud je ověření klienta povinné.
6. Server TLS ověřuje certifikát klienta. Další informace viz téma “Jak TLS poskytuje identifikaci, ověření, důvěrnost a integritu” na stránce 20.
7. Klient TLS odešle serveru zprávu "dokončeno" , která je šifrována tajným klíčem, což označuje, že klientská část navázání komunikace je dokončena.
8. Server TLS odešle klientovi zprávu "dokončeno" , která je šifrována tajným klíčem, což označuje, že část serveru navázání komunikace je dokončena.
9. Po dobu trvání relace TLS mohou nyní server a klient vyměňovat zprávy, které jsou symetricky šifrovány se sdíleným tajným klíčem.

Obrázek 5 na stránce 19 ilustruje navázání komunikace TLS.



Obrázek 5. Přehled navázání komunikace TLS

Jak TLS poskytuje identifikaci, ověření, důvěrnost a integritu

Během ověřování klienta i serveru existuje krok, který vyžaduje, aby byla data zašifrována jedním z klíčů v asymetrické dvojici klíčů a dešifrována druhým klíčem dvojice. Kód digest zprávy se používá k zajištění integrity.

Přehled kroků zahrnutých do navázání komunikace TLS naleznete v části “Přehled navázání komunikace SSL/TLS” na stránce 18.

Jak TLS poskytuje ověření

Pro ověření serveru klient používá veřejný klíč serveru k šifrování dat, která se používají k výpočtu tajného klíče. Server může generovat tajný klíč pouze v případě, že může dešifrovat data se správným soukromým klíčem. Samotný náhodný bajtový řetězec je šifrován pomocí veřejného klíče serveru (krok “4” na stránce 19 v přehledu).

Pro ověření klienta server používá veřejný klíč v certifikátu klienta k dešifrování dat, která klient odesílá během kroku “5” na stránce 19 navázání komunikace. Výměna dokončených zpráv, které jsou šifrovány pomocí tajného klíče (kroky “7” na stránce 19 a “8” na stránce 19 v přehledu), potvrzuje, že je ověření dokončeno.

Pokud se kterýkoli z kroků ověření nezdaří, navázání komunikace se nezdaří a relace se ukončí.

Výměna digitálních certifikátů během navázání komunikace TLS je součástí procesu ověření. Další informace o tom, jak certifikáty poskytují ochranu před zosobněním, naleznete v souvisejících informacích. Požadované certifikáty jsou následující, kde certifikační autorita X vydá certifikát klientovi TLS a certifikační autorita Y vydá certifikát serveru TLS:

Pouze pro ověření serveru potřebuje server TLS:

- Osobní certifikát vydaný serveru certifikační autoritou Y
- Soukromý klíč serveru

a klient TLS potřebuje:

- Certifikát certifikační autority pro certifikační autoritu Y

Pokud server TLS vyžaduje ověření klienta, server ověří identitu klienta ověřením digitálního certifikátu klienta s veřejným klíčem pro CA, která vydala osobní certifikát klientovi, v tomto případě CA X. Pro ověření serveru i klienta server potřebuje:

- Osobní certifikát vydaný serveru certifikační autoritou Y
- Soukromý klíč serveru
- Certifikát certifikační autority pro certifikační autoritu X

a klient potřebuje:

- Osobní certifikát vydaný klientovi certifikační autoritou X
- Soukromý klíč klienta
- Certifikát certifikační autority pro certifikační autoritu Y

Server TLS i klient mohou k vytvoření řetězu certifikátů pro kořenový certifikát CA potřebovat další certifikáty CA. Další informace o řetězech certifikátů naleznete v souvisejících informacích.

Co se stane během ověřování certifikátu

Jak je uvedeno v krocích “3” na stránce 19 a “6” na stránce 19 přehledu, klient TLS ověří certifikát serveru a server TLS ověří certifikát klienta. Toto ověření má čtyři aspekty:

1. Digitální podpis je zkontrolován (viz “Digitální podpisy v SSL/TLS” na stránce 22).
2. Řetěz certifikátů je kontrolován; měli byste mít přechodné certifikáty CA (viz “Jak fungují řetězy certifikátů” na stránce 16).
3. Kontrolují se data vypršení platnosti a aktivace a doba platnosti.

4. Stav odvolání certifikátu je zkontrolován (viz “Práce se zrušenými certifikáty” na stránce 359).

Resetování tajného klíče

Během navázání komunikace TLS je vygenerován *tajný klíč* pro šifrování dat mezi klientem TLS a serverem. Tajný klíč se používá v matematickém vzorci, který se použije na data k transformaci prostého textu na nečitelný šifrovaný text a šifrovaný text na prostý text.

Tajný klíč je generován z náhodného textu odeslaného jako součást navázání komunikace a používá se k šifrování prostého textu do šifrovaného textu. Tajný klíč se také používá v algoritmu MAC (Message Authentication Code), který se používá k určení, zda byla zpráva pozměněna. Další informace viz “Výtahy zpráv a digitální podpisy” na stránce 12.

Je-li zjištěn tajný klíč, prostý text zprávy by mohl být dešifrovaný z šifrovaného textu, nebo by mohl být vypočítán kód digest zprávy, což by umožnilo změnit zprávy bez detekce. Dokonce i pro složitý algoritmus, prostý text může být nakonec objeven použitím všech možných matematických transformace na ciphertext. Chcete-li minimalizovat množství dat, která lze dešifrovat nebo pozměnit, pokud je tajný klíč porušen, lze tajný klíč pravidelně znovu vyjednávat. Když byl tajný klíč znovu vyjednán, předchozí tajný klíč již nelze použít k dešifrování dat zašifrovaných novým tajným klíčem.

Jak TLS poskytuje důvěrnost

Protokol TLS používá k zajištění soukromí zpráv kombinaci symetrického a asymetrického šifrování. Během navázání komunikace TLS klient a server TLS souhlasí s šifrovacím algoritmem a sdíleným tajným klíčem, který se má použít pouze pro jednu relaci. Všechny zprávy přenášené mezi klientem TLS a serverem jsou šifrovány pomocí tohoto algoritmu a klíče, což zajišťuje, že zpráva zůstane soukromá, i když je zachycena. Vzhledem k tomu, že protokol TLS používá při přenosu sdíleného tajného klíče asymetrické šifrování, nedochází k problému s distribucí klíče. Další informace o technikách šifrování viz “Šifrování” na stránce 11.

Jak TLS poskytuje integritu

Protokol TLS poskytuje integritu dat výpočtem kódu digest zprávy. Další informace jsou uvedeny v tématu “Integrita dat zpráv” na stránce 494.

Použití TLS zajišťuje integritu dat za předpokladu, že CipherSpec v definici kanálu používá hašovací algoritmus, jak je popsáno v tabulce v části “Povolení CipherSpecs” na stránce 438.

Zejména pokud se jedná o integritu dat, měli byste se vyvarovat výběru CipherSpec , jejíž hašovací algoritmus je uveden jako "Žádný". Použití MD5 je také silně odrazováno, protože je nyní velmi staré a pro většinu praktických účelů již není bezpečné.

CipherSpecs a CipherSuites

Šifrovací bezpečnostní protokoly se musí dohodnout na algoritmech používaných zabezpečeným připojením. CipherSpecs a CipherSuites definují specifické kombinace algoritmů.

CipherSpec identifikuje kombinaci šifrovacího algoritmu a algoritmu MAC (Message Authentication Code). Oba konce připojení TLS se musí dohodnout na stejné CipherSpec , aby bylo možné komunikovat.

Produkt IBM MQ podporuje protokoly TLS1.3 a TLS1.2 a CipherSpecs. V případě potřeby však můžete povolit zamítnuté specifikace CipherSpecs.

See “Povolení CipherSpecs” na stránce 438 for information on:

- CipherSpecs podporované produktem IBM MQ
- Jak povolit zamítnuté specifikace SSL 3.0 a TLS 1.0 CipherSpecs

Důležité: Při práci s kanály IBM MQ používáte specifikaci CipherSpec. Při práci s kanály Java , JMS nebo kanály MQTT uvádíte CipherSuite.

Další informace o specifikacích CipherSpecsviz “Povolení CipherSpecs” na stránce 438.

CipherSuite je sada šifrovacích algoritmů používaných připojením TLS. Sada se skládá ze tří různých algoritmů:

- Algoritmus výměny klíčů a ověřování používaný během navázání komunikace.
- Šifrovací algoritmus použitý k zašifrování dat
- Algoritmus MAC (Message Authentication Code) použitý ke generování kódu digest zprávy

Pro každou komponentu sady existuje několik voleb, ale pouze určité kombinace jsou platné, když jsou určeny pro připojení TLS. Název platné sady CipherSuite definuje použitou kombinaci algoritmů. Například CipherSuite TLS_RSA_WITH_AES_128_CBC_SHA uvádí:

- Algoritmus výměny klíčů a ověřování RSA
- Šifrovací algoritmus AES používající režim CBC (128bitový klíč a šifrovací blok)
- Ověřovací kód zprávy SHA-1 (MAC)

Digitální podpisy v SSL/TLS

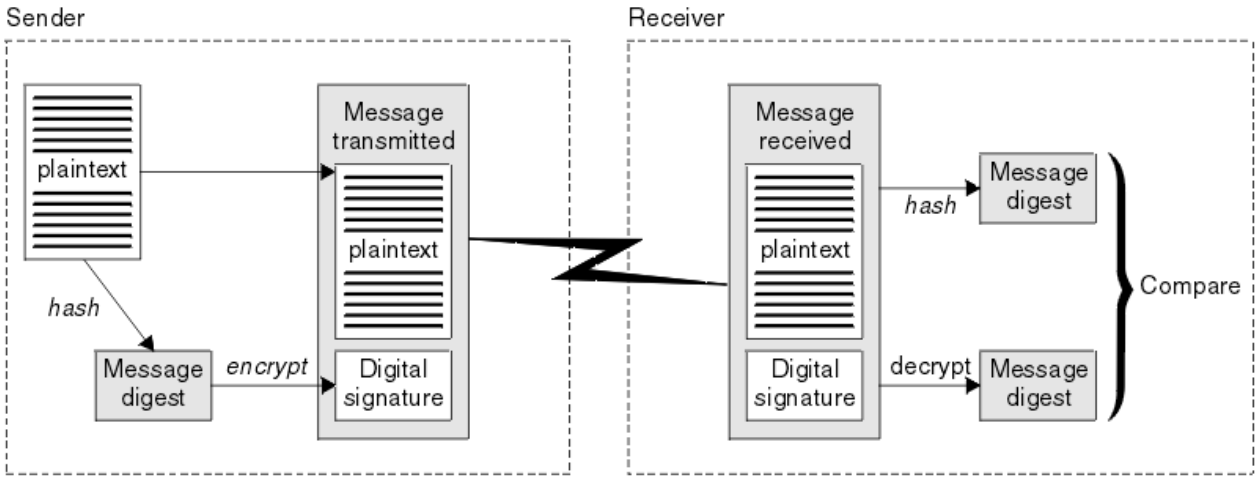
Digitální podpis je tvořen šifrováním reprezentace zprávy. Šifrování používá soukromý klíč signatáře a z důvodu efektivity obvykle pracuje na kódu digest zprávy, nikoli na zprávě samotné.

Digitální podpisy se liší podle podepsaných dat, na rozdíl od ručně psaných podpisů, které nezávisí na obsahu podepsaného dokumentu. Pokud jsou dvě různé zprávy digitálně podepsány stejnou entitou, oba podpisy se liší, ale oba podpisy lze ověřit pomocí stejného veřejného klíče, tj. veřejného klíče entity, která podepsala zprávy.

Kroky procesu digitálního podpisu jsou následující:

1. Odesílatel vypočítá kód digest zprávy a poté zašifruje kód digest pomocí soukromého klíče odesilatele a vytvoří digitální podpis.
2. Odesílatel odešle digitální podpis se zprávou.
3. Příjemce dešifruje digitální podpis pomocí veřejného klíče odesilatele a znovu vygeneruje kód digest zprávy odesilatele.
4. Příjemce vypočítá kód digest zprávy z přijatých dat zprávy a ověří, zda jsou tyto dva typy digest stejné.

Obrázek 6 na stránce 22 ilustruje tento proces.



Obrázek 6. Proces digitálního podpisu

Pokud je digitální podpis ověřen, příjemce ví, že:

- Zpráva nebyla během přenosu upravena.
- Zpráva byla odeslána entitou, která tvrdí, že ji odeslala.

Digitální podpisy jsou součástí služeb integrity a ověřování. Digitální podpisy také poskytují doklad o původu. Pouze odesílatel zná soukromý klíč, který poskytuje přesvědčivé důkazy o tom, že odesílatel je původcem zprávy.

Poznámka: Můžete také zašifrovat samotnou zprávu, která chrání důvěrnost informací ve zprávě.

Federální standardy zpracování informací

Americká vláda poskytuje technické poradenství v oblasti IT systémů a bezpečnosti, včetně šifrování dat. Národní institut pro normy a technologie (NIST) je důležitým orgánem, který se zabývá IT systémy a bezpečností. NIST vytváří doporučení a standardy, včetně standardů FIPS (Federal Information Processing Standards).

Důležitým z těchto standardů je standard FIPS 140-2, který vyžaduje použití silných šifrovacích algoritmů. Standard FIPS 140-2 také uvádí požadavky na hašovací algoritmy, které se mají použít k ochraně paketů před úpravami při přenosu.

Poznámka: V systému AIX, Linux, and Windowsposkytuje produkt IBM MQ kompatibilitu se standardem FIPS 140-2 prostřednictvím šifrovacího modulu IBM Crypto for C (ICC) . Certifikát pro tento modul byl přesunut do historického stavu. Zákazníci by si měli prohlédnout IBM Crypto for C (ICC) certifikát a měli by si být vědomi všech doporučení poskytnutých NIST. Náhradní modul FIPS 140-3 momentálně probíhá a jeho stav lze zobrazit jeho vyhledáním v modulech NIST CMVP v seznamu procesů.

Produkt IBM MQ poskytuje podporu FIPS 140-2, pokud k tomu byl nakonfigurován.

V průběhu času analytici vyvíjejí útoky proti existujícím šifrovacím a hašovací algoritmům. Nové algoritmy jsou přijaty, aby odolaly těmto útokům. Standard FIPS 140-2 je pravidelně aktualizován, aby zohledňoval tyto změny.

Související pojmy

“Národní bezpečnostní agentura (NSA) Suite B kryptografie” na stránce 23
Vláda Spojených států amerických poskytuje technické poradenství v oblasti systémů IT a bezpečnosti, včetně šifrování dat. Americká národní bezpečnostní agentura (NSA) doporučuje ve svém standardu Suite B sadu interoperabilních šifrovacích algoritmů.

Národní bezpečnostní agentura (NSA) Suite B kryptografie

Vláda Spojených států amerických poskytuje technické poradenství v oblasti systémů IT a bezpečnosti, včetně šifrování dat. Americká národní bezpečnostní agentura (NSA) doporučuje ve svém standardu Suite B sadu interoperabilních šifrovacích algoritmů.

Standard Suite B určuje provozní režim, ve kterém se používá pouze specifická sada zabezpečených šifrovacích algoritmů. Standard Suite B specifikuje:

- Šifrovací algoritmus (AES)
- Algoritmus výměny klíčů (Elliptic Curve Diffie-Hellman, také známý jako ECDH)
- Algoritmus digitálního podpisu (Elliptic Curve Digital Signature Algorithm, také známý jako ECDSA)
- Hašovací algoritmy (SHA-256 nebo SHA-384)

Kromě toho standard IETF RFC 6460 specifikuje profily vyhovující standardu Suite B, které definují podrobnou konfiguraci aplikace a chování nezbytné pro splnění standardu Suite B. Definuje dva profily:

1. Profil vyhovující standardu Suite B pro použití s protokolem TLS 1.2. Při konfiguraci pro operaci vyhovující standardu Suite B se používá pouze omezená sada uvedených šifrovacích algoritmů.
2. Přechodný profil pro použití s protokolem TLS 1.0 nebo TLS 1.1. Tento profil umožňuje interoperabilitu se servery, které nejsou kompatibilní se standardem Suite B. Při konfiguraci pro přechodnou operaci Suite B lze použít další šifrovací a hašovací algoritmy.

Standard Suite B je koncepčně podobný standardu FIPS 140-2, protože omezuje sadu povolených šifrovacích algoritmů, aby poskytoval zajištěnou úroveň zabezpečení.

Na systémech AIX, Linux, and Windows IBM MQlze konfigurovat tak, aby vyhovovaly profilu TLS 1.2 kompatibilnímu se standardem Suite B, ale nepodporuje přechodný profil Suite B. Další informace uvádí téma “Šifrování NSA Suite B v IBM MQ” na stránce 41.

Související odkazy

“Federální standardy zpracování informací” na stránce 23
Americká vláda poskytuje technické poradenství v oblasti IT systémů a bezpečnosti, včetně šifrování dat. Národní institut pro normy a technologie (NIST) je důležitým orgánem, který se zabývá IT systémy a bezpečností. NIST vytváří doporučení a standardy, včetně standardů FIPS (Federal Information Processing Standards).

IBM MQ mechanismy zabezpečení

Tato kolekce témat popisuje specifické mechanizmy v produktu IBM MQ , které implementují různé koncepce zabezpečení.

Protokoly zabezpečení TLS v adresáři IBM MQ

Produkt IBM MQ podporuje protokol TLS (Transport Layer Security), který poskytuje zabezpečení na úrovni propojení pro kanály zpráv a kanály MQI.

Kanály zpráv a kanály MQI mohou používat protokol TLS k zajištění zabezpečení na úrovni propojení. Volající MCA je klient TLS a odpovídající MCA je server TLS.

Produkt IBM MQ podporuje verze 1.2 a 1.3 protokolu TLS. Starší verze TLS, stejně jako SSL, nejsou standardně povoleny, ale mohou být v případě potřeby. Šifrovací algoritmy používané protokolem TLS lze určit zadáním CipherSpec jako součást definice kanálu.

Seznam CipherSpecs podporovaných produkty IBM MQ a “Zamítnuté specifikace CipherSpecs” na stránce 453 pro zamítnuté položky naleznete v části “Povolení CipherSpecs” na stránce 438 .

Pomocí parametrů SECPROT a SSLCIPH můžete zobrazit protokol zabezpečení a specifikaci CipherSpec používanými v kanálu.

Na každém konci kanálu zpráv a na konci serveru kanálu MQI jedná agent MCA jménem správce front, ke kterému je připojen. Během navázání komunikace TLS odešle agent MCA digitální certifikát správce front partnerskému adaptéru MCA na druhém konci kanálu. Kód IBM MQ na konci klienta kanálu MQI jedná jménem uživatele klientské aplikace IBM MQ . Během navazování komunikace TLS kód IBM MQ odešle digitální certifikát uživatele do agenta MCA na konci serveru kanálu MQI.

Správci front a uživatelé klienta IBM MQ nemusí mít osobní digitální certifikáty přidružené k nim, pokud vystupují jako klienti TLS, pokud není na straně serveru kanálu určeno SSLCAUTH (REQUIRED).

Digitální certifikáty jsou uloženy v *úložišti klíčů*. Atribut správce front **SSLKeyRepository** určuje umístění úložiště klíčů, které obsahuje digitální certifikát správce front. V klientském systému IBM MQ proměnná prostředí MQSSLKEYR určuje umístění úložiště klíčů, které obsahuje digitální certifikát uživatele. Alternativně může klientská aplikace IBM MQ určit své umístění v poli **KeyRepository** struktury voleb konfigurace TLS MQSCO ve volání MQCONNX. Další informace o klíčových úložištích a o jejich umístění naleznete v souvisejících tématech.

Podpora pro TLS

Produkt IBM MQ poskytuje podporu pro protokoly TLS 1.2 a TLS 1.3 na všech platformách. Další informace o protokolu TLS naleznete v informacích v dílčích tématech.

Klienti Java a JMS
Tito klienti používají prostředí JVM k poskytování podpory TLS.

AIX, Linux, and Windows
Podpora TLS je nainstalována s produktem IBM MQ.

IBM i
Podpora TLS je nedílnou součástí operačního systému IBM i .

z/OS

Podpora TLS je nedílnou součástí operačního systému z/OS . Podpora TLS v systému z/OS se nazývá *System SSL*.

Chcete-li získat informace o předpokladech pro podporu TLS v produktu IBM MQ , prohlédněte si téma Systémové požadavky pro IBM MQ.

Související pojmy

“Šifrovací bezpečnostní protokoly: TLS” na stránce 18

Šifrovací protokoly poskytují zabezpečená připojení, což umožňuje dvěma stranám komunikovat se soukromím a integritou dat. Protokol TLS (Transport Layer Security) se vyvinul z protokolu SSL (Secure Sockets Layer). Produkt IBM MQ podporuje protokol TLS.

Úložiště klíčů SSL/TLS

Vzájemně ověřené připojení TLS vyžaduje úložiště klíčů na každém konci připojení. Úložiště klíčů obsahuje digitální certifikáty a soukromé klíče.

Tyto informace používají obecný termín *úložiště klíčů* k popisu úložiště digitálních certifikátů a jejich přidružených soukromých klíčů. Na úložiště klíčů se odkazují různé názvy na různých platformách a prostředích, která podporují TLS:

- IBM i V systému IBM i: *úložiště certifikátů*
- V systémech Java a JMS: *keystore* a *truststore* .
- ALW V systému AIX, Linux, and Windows: *soubor databáze klíčů*
- z/OS V systému z/OS: *keyring*

Další informace naleznete v tématech “digitální certifikáty” na stránce 13 a “Koncepce TLS (Transport Layer Security)” na stránce 18.

Vzájemně ověřené připojení TLS vyžaduje úložiště klíčů na každém konci připojení. Úložiště klíčů může obsahovat následující certifikáty a požadavky:

- Počet certifikátů CA od různých certifikačních autorit, které umožňují správci front nebo klientovi ověřit certifikáty, které obdrží od svého partnera na vzdáleném konci připojení. Jednotlivé certifikáty mohou být v řetězu certifikátů.
- Jeden nebo více osobních certifikátů přijatých od certifikační autority. Ke každému správci front nebo k produktu IBM MQ MQI clientpřidružíte samostatný osobní certifikát. Osobní certifikáty jsou nezbytné pro klienta TLS, pokud je vyžadováno vzájemné ověření. Pokud není vyžadováno vzájemné ověření, osobní certifikáty nejsou na klientovi potřebné. Úložiště klíčů může také obsahovat soukromý klíč odpovídající jednotlivým osobním certifikátům.
- Požadavky na certifikáty, které čekají na podepsání důvěryhodným certifikátem CA.

Další informace o ochraně úložiště klíčů viz “Ochrana úložišť klíčů IBM MQ” na stránce 26.

Umístění úložiště klíčů závisí na platformě, kterou používáte:

IBM i **IBM i**

Úložiště klíčů je úložiště certifikátů. Výchozí úložiště certifikátů systému je umístěno v adresáři `/QIBM/UserData/ICSS/Cert/Server/Default` v integrovaném systému souborů (IFS). Produkt IBM MQ ukládá heslo pro úložiště certifikátů do *souboru pro uložení hesla*. Například soubor pro dočasné ukládání pro správce front `QM1` je `/QIBM/UserData/mqm/qmgrs/QM1/ssl/Stash.sth`.

Alternativně můžete určit, že má být místo toho použito systémové úložiště certifikátů IBM i . Chcete-li to provést, změňte hodnotu atributu **SSLKEYR** správce front na `*SYSTEM`. Tato hodnota označuje, že správce front musí používat úložiště certifikátů systému a že je správce front registrován pro použití jako aplikace s produktem DCM (Digital Certificate Manager).

Úložiště certifikátů také obsahuje soukromý klíč pro správce front.

Systémy AIX, Linux, and Windows

Úložiště klíčů je soubor databáze klíčů. Například v systému AIX and Linuxje výchozí soubor databáze klíčů pro správce front `QM1` `/var/mqm/qmgrs/QM1/ssl/key.kdb`. Pokud je produkt IBM MQ nainstalován ve výchozím umístění, ekvivalentní cesta v systému Windows je `C:\ProgramData\IBM\MQ\Qmgrs\QM1\ssl\key.kdb`.

V 9.3.0 Pro přístup k souboru databáze klíčů IBM MQ musí být zadáno heslo pro databázi klíčů. To lze provést buď přímo, nebo prostřednictvím souboru pro uložení hesla. Je-li použit soubor pro dočasné ukládání hesla, musí být ve stejném adresáři a musí mít stejný systém souborů jako databáze klíčů a musí končit příponou `.sth`, například `/var/mqm/qmgrs/QM1/ssl/key.sth`.

Poznámka: Šifrovací hardwarové karty PKCS #11 mohou obsahovat certifikáty a klíče, které jsou jinak uloženy v souboru databáze klíčů. Když jsou certifikáty a klíče drženy na kartách PKCS #11 , produkt IBM MQ stále vyžaduje přístup jak k souboru databáze klíčů, tak k souboru hesel.

V systémech AIX, Linux, and Windows obsahuje databáze klíčů také soukromý klíč pro osobní certifikát přidružený ke správci front nebo k produktu IBM MQ MQI client.

z/OS

Certifikáty jsou drženy ve svazku klíčů v produktu z/OS.

Další externí správci zabezpečení (ESM) také používají svazky klíčů pro ukládání certifikátů.

Soukromé klíče jsou spravovány produktem RACF.

Ochrana úložišť klíčů IBM MQ

Úložiště klíčů pro IBM MQ je soubor. Ujistěte se, že k souboru úložiště klíčů má přístup pouze zamýšlený uživatel. Tím zabráníte tomu, aby narušitel nebo jiný neoprávněný uživatel kopíroval soubor úložiště klíčů do jiného systému a poté nastavil identické ID uživatele v tomto systému, aby zosobňoval zamýšleného uživatele.

Oprávnění k souborům závisí na umask uživatele a na použitém nástroji. V systému Windowsúčty IBM MQ vyžadují oprávnění `BypassTraverseChecking` , což znamená, že oprávnění složek v cestě k souboru nemají žádný vliv.

Zkontrolujte oprávnění souborů úložiště klíčů a ujistěte se, že soubory a obsahující složky nejsou čitelné pro celý svět, nejlépe ani pro skupiny.

Nastavení úložiště klíčů jen pro čtení je dobrým zvykem, ať už používáte jakýkoli systém, přičemž pouze administrátor může povolit operace zápisu, aby mohl provádět údržbu.

V praxi musíte chránit všechna úložiště klíčů bez ohledu na umístění a bez ohledu na to, zda jsou chráněna heslem či nikoli; chránit úložiště klíčů.

Digitální štítky certifikátů, pochopení požadavků

Při nastavování protokolu TLS pro použití digitálních certifikátů mohou existovat specifické požadavky na označení, které musíte dodržovat, v závislosti na použité platformě a metodě, kterou používáte pro připojení.

Co je to označení certifikátu?

Popisek certifikátu je jedinečný identifikátor představující digitální certifikát uložený v úložišti klíčů a poskytuje pohodlný název čitelný pro člověka, s nímž lze při provádění funkcí správy klíčů odkazovat na konkrétní certifikát. Popisek certifikátu přiřadíte při prvním přidání certifikátu do úložiště klíčů.

Popisek certifikátu je oddělen od polí **`Subject Distinguished Name`** nebo **`Subject Common Name`** certifikátu. Všimněte si, že **`Subject Distinguished Name`** a **`Subject Common Name`** jsou pole v samotném certifikátu. Ty jsou definovány při vytvoření certifikátu a nelze je změnit. V případě potřeby však můžete změnit popisek přidružený k digitálnímu certifikátu.

Syntaxe popisku certifikátu

Popisek certifikátu může obsahovat písmena, čísla a interpunkci s následujícími podmínkami:

- Multi Popisek certifikátu může obsahovat až 64 znaků.
- z/OS Popisek certifikátu může obsahovat až 32 znaků.
- Popisek certifikátu může obsahovat mezery.
- Popisky rozlišují velká a malá písmena.
- V systémech, které používají EBCDIC katakana, nemůžete používat malá písmena.

Další požadavky na hodnoty popisků certifikátů jsou uvedeny v následujících sekcích.

Jak se používá označení certifikátu?

Produkt IBM MQ používá popisky certifikátů k vyhledání osobního certifikátu, který je odeslán během navázání komunikace TLS. To eliminuje nejednoznačnost, pokud v úložišti klíčů existuje více než jeden osobní certifikát.

Popisek certifikátu můžete nastavit na vámi zvolenou hodnotu. Pokud nenastavíte hodnotu, použije se výchozí popisek, který se řídí konvencí pojmenování v závislosti na platformě, kterou používáte. Podrobnosti naleznete v následujících sekcích, které se týkají konkrétních platforem.

Notes:

1. Popisek certifikátu nemůžete nastavit sami na systémech Java nebo JMS .
2. Automaticky definované kanály vytvořené uživatelskou procedurou automatické definice kanálu (CHAD) nemohou nastavit popisek certifikátu, protože k navázání komunikace TLS došlo v době vytvoření kanálu. Nastavení popisku certifikátu v uživatelské proceduře CHAD pro příchozí kanály nemá žádný vliv.

V tomto kontextu klient TLS odkazuje na partnera připojení, který zahajuje navázání komunikace, což může být klient IBM MQ nebo jiný správce front.

Během navázání komunikace TLS klient TLS vždy získá a ověří digitální certifikát od serveru.
S implementací IBM MQ si server TLS vždy vyžádá certifikát od klienta a klient vždy poskytne certifikát serveru, pokud je nalezen. Pokud klient nemůže najít osobní certifikát, odešle na server odpověď no `certificate` .

Server TLS vždy ověřuje certifikát klienta, pokud je odeslán. Pokud klient neodešle certifikát, ověření se nezdaří, pokud je konec kanálu, který vystupuje jako server TLS, definován buď s parametrem **SSLCAUTH** nastaveným na hodnotu *REQUIRED* , nebo s nastavenou hodnotou parametru **SSLPEER** .

Povšimněte si, že příchozí kanály (včetně kanálů příjemce, žadatele, příjemce klastru, nekvalifikovaného serveru a připojení serveru) odesílají konfigurovaný certifikát pouze v případě, že verze produktu IBM MQ vzdáleného partnera plně podporuje konfiguraci popisku certifikátu a kanál používá protokol TLS CipherSpec.

Nekvalifikovaný kanál serveru je kanál, který nemá nastaveno pole CONNAME.

Ve všech ostatních případech parametr **CERTLABL** správce front určuje odeslaný certifikát. Bez ohledu na nastavení popisku specifické pro konkrétní kanál obdrží certifikát konfigurovaný parametrem **CERTLABL** správce front pouze následující:

- Klienti Java a JMS podporující SNI (Server Name Indication), tj. certifikáty pro jednotlivé kanály.
- Verze IBM MQ před IBM MQ 8.0.
- Spravovaní klienti .NET

Kromě toho musí být certifikát používaný kanálem vhodný pro kanál CipherSpec -další informace naleznete v části “Digitální certifikáty a kompatibilita CipherSpec v produktu IBM MQ” na stránce 46 .

Produkt IBM MQ 8.0 a novější podporují použití více certifikátů ve stejném správci front s použitím popisku certifikátu pro jednotlivé kanály určeného pomocí atributu **CERTLABL** v definici kanálu. Příchozí

kanály do správce front (například připojení k serveru nebo příjemce) spoléhají na zjištění názvu kanálu pomocí SNI (TLS Server Name Indication), aby bylo možné předložit správný certifikát ze správce front. Další informace o použití více certifikátů ve správci front viz “Jak produkt IBM MQ poskytuje schopnost více certifikátů” na stránce 29.

Pokud se kanál připojuje ke správci cílové fronty prostřednictvím IBM MQ Internet Pass-Thru (MQIPT) a trasa MQIPT má nastaveny obě hodnoty **SSLServer** a **SSLClient** , existují mezi koncovými body dvě oddělené relace TLS. Ve verzích starších než IBM MQ 9.2.5data SNI netečou přes přerušení relace. Tím zabráníte použití certifikátu pro jednotlivé kanály ve správci cílové fronty pro připojení TLS mezi produktem MQIPT a správcem front. V produktu IBM MQ 9.2.5lze produkt MQIPT konfigurovat tak, aby umožňoval použití více certifikátů správcem cílové fronty, a to buď nastavením SNI na název kanálu, nebo předáním SNI přijatého v příchozím připojení k přenosové cestě. Další informace o podpoře více certifikátů a MQIPTnaleznete v tématu IBM MQ Podpora více certifikátů s produktem MQIPT.

Další informace o připojení správce front pomocí jednosměrného ověřování, tj. pokud klient TLS neodešle certifikát, naleznete v tématu Připojení dvou správců front pomocí jednosměrného ověřování.

Systémy pro více platforem

Multi

V systému Multiplatformsodešle server TLS klientovi certifikát.

Pro správce front a klienty jsou v následujícím pořadí prohledávány hodnoty, které nejsou prázdné. První neprázdná hodnota určuje popisek certifikátu. Popisek certifikátu musí existovat v úložišti klíčů. Pokud není nalezen odpovídající certifikát ve správném velikosti a formátu, který by odpovídal popisku, dojde k chybě a navázání komunikace TLS se nezdaří.

Správci front

1. Atribut popisku certifikátu kanálu **CERTLABL**.
2. Atribut popisku certifikátu správce front **CERTLABL**.
3. Výchozí hodnota, která je ve formátu: `ibmwebspheremq` s připojeným názvem správce front, vše malými písmeny. Například pro správce front s názvem `QM1`je výchozí popisek certifikátu `ibmwebspheremqqm1`.

IBM MQ klienti

1. Atribut popisku certifikátu **CERTLABL** v definici kanálu CLNTCONN.
2. Atribut struktury MQSCO **CertificateLabel** .
3. Proměnná prostředí **MQCERTLABL**.
4. Atribut klienta `.ini` file (v jeho sekci SSL) **CertificateLabel**
5. Výchozí nastavení, které je ve formátu: `ibmwebspheremq` s ID uživatele, které aplikace klienta spouští jako připojené, vše malými písmeny. Například pro ID uživatele USER1je výchozí popisek certifikátu `ibmwebspheremquser1`.

z/OS systémy

z/OS

IBM MQ Klienti nejsou v systému z/OSpodporováni. Správce front z/OS však může jednat v roli klienta TLS při inicializaci připojení nebo serveru TLS při přijímání požadavku na připojení. Požadavky na popisek certifikátu pro správce front produktu z/OS platí v obou těchto rolích a liší se od požadavků na systému Multiplatforms.

Pro správce front a klienty jsou v následujícím pořadí prohledávány hodnoty, které nejsou prázdné. První neprázdná hodnota určuje popisek certifikátu. Popisek certifikátu musí existovat v úložišti klíčů. Pokud není nalezen odpovídající certifikát ve správném velikosti a formátu, který by odpovídal popisku, dojde k chybě a navázání komunikace TLS se nezdaří.

1. Atribut popisku certifikátu kanálu, **CERTLABL**.

2. V případě sdílení se jedná o atribut popisku certifikátu skupiny sdílení front **CERTQSGL**.

   Není-li sdílený, atribut popisku certifikátu správce front **CERTLABL**.
3. Výchozí nastavení ve formátu: `ibmWebSphereMQ` s připojeným názvem správce front nebo skupiny sdílení front. Všimněte si, že tento řetězec rozlišuje velikost písmen a musí být zapsán tak, jak je uvedeno. Například pro správce front s názvem `QM1`je výchozí popisek certifikátu `ibmWebSphereMQQM1`.
4. Pokud není nalezen certifikát s formátem ve volbě "3" na stránce 29, IBM MQ se pokusí použít certifikát označený jako výchozí v svazku klíčů.

Informace o zobrazení úložiště klíčů viz "Vyhledání úložiště klíčů pro správce front v systému z/OS" na stránce 333.

Klienti IBM MQ Java a IBM MQ JMS

Klienti IBM MQ Java a IBM MQ JMS používají prostředky svého poskytovatele rozšíření JSSE (Java Secure Socket Extension) k výběru osobního certifikátu během navázání komunikace TLS, a proto nepodléhají požadavkům na označení certifikátu.

Výchozí chování je, že klient JSSE prochází certifikáty v úložišti klíčů a vybírá první nalezený přijatelný osobní certifikát. Toto chování je však pouze výchozí a závisí na implementaci poskytovatele JSSE.

Kromě toho je rozhraní JSSE vysoce přizpůsobitelné prostřednictvím konfigurace a přímého přístupu aplikace za běhu. Specifické podrobnosti naleznete v dokumentaci dodané poskytovatelem rozhraní JSSE.

Chcete-li odstranit problémy nebo lépe porozumět navázání komunikace prováděnému klientskou aplikací IBM MQ Java v kombinaci se specifickým poskytovatelem JSSE, můžete povolit ladění nastavením `javax.net.debug=ssl` v prostředí JVM.

Proměnnou v rámci aplikace můžete nastavit pomocí konfigurace nebo zadáním příkazu `-Djavax.net.debug=ssl` na příkazovém řádku.

Linux *Jak produkt IBM MQ poskytuje schopnost více certifikátů*

SNI (Server Name Indikace) je rozšíření protokolu TLS, které umožňuje klientovi označit, jakou službu vyžaduje. V terminologii IBM MQ se to rovná kanálu.

Rozšíření SNI používá produkt IBM MQ k povolení zadání více certifikátů v různých kanálech pomocí parametru CERTLABL v definici kanálu.

Adresa SNI použitá produktem IBM MQ je založena na požadovaném názvu kanálu následovaném příponou `.chl.mq.ibm.com`.

Názvy kanálů IBM MQ jsou mapovány na platné názvy SNI následujícím způsobem:

- Velká písmena A až Z jsou přeložena na malá písmena.
- Číslice `0` až `9` zůstávají beze změny.
- Všechny ostatní znaky, včetně malých písmen a na `z`, jsou převedeny na dvouciferný hexadecimální kód ASCII (malými písmeny) následovaný pomlčkou.
  - Malá písmena a na z mapovat na hexadecimální `61-` na `7a-` v uvedeném pořadí
  - procento (%) se mapuje na hexadecimální `25-`
  - pomlčka (-) se mapuje na hexadecimální `2d-`
  - tečka (`.`) se mapuje na hexadecimální `2e-`
  - dopředné lomítko (/) se mapuje na hexadecimální `2f-`
  - podtržítko (_) se mapuje na hexadecimální `5f-`

Na platformách EBCDIC je název kanálu před použitím tohoto mapování převeden na ASCII.

Například název kanálu `TO.QMGR1` se mapuje na adresu SNI `to2e-qmgr1.chl.mq.ibm.com`.

Naproti tomu název kanálu s malými písmeny `to.qmgr1` se mapuje na adresu SNI `74-6f-2e-71-6d-67-72-1.chl.mq.ibm.com`.

Poznámka: V prostředích, kde generovaná adresa URL SNI musí odpovídat specifikacím formátování adres URL, například když se klient připojuje ke správci front spuštěnému v produktu Red Hat® OpenShift® přes trasu Red Hat OpenShift , nesmí název kanálu končit malým písmenem.

Vlastnost **OutboundSNI** sekce SSL vám umožňuje vybrat, zda by měl být SNI nastaven na název cílového kanálu IBM MQ ke vzdálenému systému při inicializaci připojení TLS, nebo na název hostitele. Další informace o vlastnosti **OutboundSNI** naleznete v sekci SSL souboru qm.ini a sekci SSL konfiguračního souboru klienta.

Více certifikátů vyžaduje, aby byl SNI nastaven na název kanálu IBM MQ . Pokud se pro připojení ke kanálu IBM MQ s nakonfigurovaným popiskem certifikátu použije název hostitele, vlastní nebo žádný SNI, bude připojující se aplikace odmítnuta s chybou MQRC_SSL_INITIALIZATION_ERROR a ve vzdálených protokolech chyb správce front se vytiskne zpráva AMQ9673 .

V 9.3.0 Pokud se kanál připojuje ke správci cílové fronty prostřednictvím IBM MQ Internet Pass-Thru (MQIPT), MQIPT musí být nakonfigurován tak, aby buď nastavil název SNI na název kanálu, nebo aby prošel SNI přijatým v příchozím připojení k trase, aby mohl cílový správce front používat více certifikátů. Další informace o podpoře více certifikátů a MQIPTnaleznete v tématu IBM MQ Podpora více certifikátů s produktem MQIPT.

Další informace o způsobu použití této vlastnosti naleznete v tématu Připojení ke správci front implementovanému v klastru Red Hat OpenShift.

Aktualizace úložiště klíčů správce front
Změníte-li obsah úložiště klíčů, existující procesy správce front nevyzvednou nový obsah, dokud nebude zadán příkaz REFRESH SECURITY TYPE (SSL) nebo dokud nebude správce front restartován.

Další informace o příkazu REFRESH SECURITY TYPE (SSL) viz REFRESH SECURITY.

Pokud správce front po změně obsahu úložiště klíčů vytvoří nový proces kanálu (pomocí `amqrmppa` nebo **runmqchl**), začne nový proces okamžitě používat nové certifikáty, zatímco existující procesy budou nadále používat svou kopii úložiště klíčů uloženou v mezipaměti. Další informace viz část “Když změny certifikátů nebo úložiště certifikátů vstoupí v platnost v systému AIX, Linux, and Windows” na stránce 307.

Všimněte si, že více spuštěných kanálů může používat různé verze úložiště klíčů, dokud nezadáte příkaz REFRESH SECURITY TYPE (SSL).

Úložiště klíčů můžete také aktualizovat pomocí příkazů PCF nebo IBM MQ Explorer. Další informace viz Příkaz MQCMD_REFRESH_SECURITY a téma *Aktualizace zabezpečení TLS* v sekci IBM MQ Explorer této dokumentace produktu.

Související pojmy
“Aktualizace pohledu klienta na obsah úložiště klíčů SSL/TLS a nastavení SSl/TLS” na stránce 30
Chcete-li aktualizovat aplikaci klienta s aktualizovaným obsahem úložiště klíčů, musíte aplikaci klienta zastavit a restartovat.

Aktualizace pohledu klienta na obsah úložiště klíčů SSL/TLS a nastavení SSl/TLS
Chcete-li aktualizovat aplikaci klienta s aktualizovaným obsahem úložiště klíčů, musíte aplikaci klienta zastavit a restartovat.

V klientu IBM MQ nelze aktualizovat zabezpečení. Pro klienty neexistuje ekvivalent příkazu REFRESH SECURITY TYPE (SSL) (viz REFRESH SECURITY). pro více informací.

Chcete-li aktualizovat klientskou aplikaci s aktualizovaným obsahem úložiště klíčů, musíte zastavit a znovu spustit aplikaci, kdykoli změníte bezpečnostní certifikát.

Pokud restartování kanálu aktualizuje konfigurace a pokud má vaše aplikace logiku opětovného připojení, je možné aktualizovat zabezpečení na klientovi zadáním příkazu STOP CHL STATUS (INACTIVE).

Související pojmy

“Aktualizace úložiště klíčů správce front” na stránce 30
Změníte-li obsah úložiště klíčů, existující procesy správce front nevyzvednou nový obsah, dokud nebude zadán příkaz REFRESH SECURITY TYPE (SSL) nebo dokud nebude správce front restartován.

Ochrana heslem MQCSP

Ověřovací pověření uvedená ve struktuře MQCSP mohou být buď chráněna pomocí funkce ochrany heslem produktu IBM MQ MQCSP, nebo šifrována pomocí šifrování TLS.

Aplikace IBM MQ client mohou při připojení ke správci front zadat ID uživatele a heslo. V 9.3.4 Od IBM MQ 9.3.4mohou aplikace také dodat token ověření jako alternativní metodu ověření. Tato pověření jsou odeslána správci front ve struktuře MQCSP.

Pokud kanál používá šifrování TLS, jsou pověření v protokolu MQCSP šifrována podle specifikace šifrování TLS. V systému IBM MQ 8.0platí, že pokud kanál nepoužívá šifrování TLS, může produkt IBM MQ tato pověření před odesláním po síti chránit, aby se zabránilo odesílání pověření po síti v prostém textu. Funkce IBM MQ , která chrání tato pověření, se nazývá ochrana pomocí hesla MQCSP.

Je-li použita ochrana heslem MQCSP, jsou chráněna následující data ve struktuře MQCSP:

- Heslo, pokud je pole `MQCSP.AuthenticationType` nastaveno na hodnotu `MQCSP_AUTH_USER_ID_AND_PW`.
- V 9.3.4 Token ověření, je-li pole `MQCSP.AuthenticationType` nastaveno na hodnotu `MQCSP_AUTH_ID_TOKEN`.

Důležité: Ochrana heslem MQCSP je užitečná pro účely testování a vývoje, protože použití ochrany heslem MQCSP je jednodušší než nastavení šifrování TLS, ale ne tak bezpečné. Pro produkční účely používejte raději šifrování TLS než ochranu heslem IBM MQ , zejména pokud je síť mezi klientem a správcem front nedůvěryhodná, protože šifrování TLS je bezpečnější.

Pokud vás zajímá, jaké šifrování se používá a kolik ochrany nabízí, musíte použít úplné šifrování TLS. Pomocí protokolu TLS jsou algoritmy veřejně známé a můžete vybrat odpovídající algoritmus pro váš podnik pomocí atributu kanálu **SSLCIPH** .

Další informace o struktuře MQCSP viz Struktura MQCSP.

Pověření ve struktuře MQCSP jsou chráněna pomocí ochrany heslem IBM MQ , pokud jsou splněny všechny následující podmínky:

- Oba konce připojení používají produkt IBM MQ 8.0nebo novější.
- Kanál nepoužívá šifrování TLS. Kanál nepoužívá šifrování TLS, pokud má prázdný atribut **SSLCIPH** nebo je atribut **SSLCIPH** nastaven na specifikaci šifrování, která neposkytuje šifrování. Šifry s hodnotou null, například NULL_SHA, neposkytují šifrování.
- Pole `MQCSP.AuthenticationType` je nastaveno na hodnotu `MQCSP_AUTH_USER_ID_AND_PWD` nebo `MQCSP_AUTH_ID_TOKEN`. Další informace o poli `MQCSP.AuthenticationType` viz **AuthenticationType**.
- Pokud je klient IBM MQ Explorer a režim kompatibility identifikace uživatele není povolen. Tento režim není výchozím režimem, který produkt IBM MQ Explorer používá k odeslání ID uživatele a hesla. Tuto podmínku lze použít pouze pro IBM MQ Explorer.

Pokud není splněna některá z těchto podmínek, nejsou pověření chráněna ochranou pomocí hesla MQCSP. Pokud hodnota atributu **PasswordProtection** zakazuje odeslání pověření v prostém textu a kanál nepoužívá šifrování TLS, připojení se nezdaří a vrátí se kód příčiny MQRC_PASSWORD_PROTECTION_ERROR (2594).

Nastavení konfigurace `PasswordProtection`

Atribut **PasswordProtection** v sekci **Channels** konfiguračních souborů klienta a správce front může zabránit odeslání pověření v prostém textu.

Poznámka: Tento atribut je relevantní pouze pro připojení, která nepoužívají šifrování TLS. Pověření jsou šifrována pomocí TLS namísto ochrany pomocí ochrany pomocí hesla MQCSP, pokud připojení používá šifrování TLS.

Atribut lze nastavit na jednu z následujících hodnot. Výchozí hodnota je `compatible`.

Kompatibilní
Pověření jsou odesílána jako prostý text, pokud správce front nebo klient používají verzi IBM MQ dřívější než IBM MQ 8.0. To znamená, že pověření lze odesílat po síti v prostém textu kvůli kompatibilitě s verzemi produktu IBM MQ , které nepodporují ochranu pomocí hesla MQCSP.

Pověření jsou chráněna ochranou pomocí hesla MQCSP, pokud správce front i klient používají verzi produktu IBM MQ na adrese IBM MQ 8.0 nebo novější.

Připojení se nezdaří před odesláním pověření, pokud správce front i klient spouští verzi produktu IBM MQ na adrese IBM MQ 8.0 nebo novější a pole `MQCSP.AuthenticationType` není nastaveno na hodnotu `MQCSP_AUTH_USER_ID_AND_PW` nebo `MQCSP_AUTH_ID_TOKEN`.

Vždy
Pověření nesmí být odeslána přes nechráněnou síť.

Pověření jsou chráněna ochranou pomocí hesla MQCSP, pokud správce front i klient používají verzi produktu IBM MQ na adrese IBM MQ 8.0 nebo novější.

Připojení se nezdaří před odesláním pověření v následujících případech:

- Pole `MQCSP.AuthenticationType` není nastaveno na `MQCSP_AUTH_USER_ID_AND_PW` nebo `MQCSP_AUTH_ID_TOKEN`.
- Ve správci front nebo v klientu je spuštěna verze IBM MQ starší než IBM MQ 8.0.

volitelné
Pověření jsou chráněna ochranou pomocí hesla MQCSP, pokud správce front i klient používají verzi produktu IBM MQ na adrese IBM MQ 8.0 nebo novější a pole `MQCSP.AuthenticationType` je nastaveno na hodnotu `MQCSP_AUTH_USER_ID_AND_PW` nebo `MQCSP_AUTH_ID_TOKEN`. Jinak se pověření odesílají jako prostý text.

varování
Každému klientovi je povoleno odeslat pověření v prostém textu. Pokud jsou přijata pověření v prostém textu, do protokolů chyb správce front se zapíše varovná zpráva AMQ9297W .

Tuto volbu lze zadat pouze v konfiguračním souboru správce front.

U klientů Java a JMS se chování atributu **`PasswordProtection`** mění v závislosti na tom, zda klient používá režim kompatibility nebo režim MQCSP:

- Pokud klienti Java a JMS pracují v režimu kompatibility, struktura MQCSP se nepoužije k odeslání ID uživatele a hesla při připojení klienta. Proto je chování atributu **`PasswordProtection`** stejné jako chování popsané pro klienty, kteří mají spuštěnou starší verzi produktu IBM MQ než IBM MQ 8.0.
- Pokud klienti Java a JMS pracují v režimu MQCSP, chování atributu **`PasswordProtection`** je takové, jak je popsáno.

Další informace o ověřování připojení s klienty Java a JMS naleznete v tématu "Ověření připojení s klientem Java" na stránce 81.

Ochrana pomocí hesla MQCSP a MQIPT

V 9.3.1

Pokud se klient připojuje ke správci front prostřednictvím IBM MQ Internet Pass-Thru (MQIPT), může být směrování MQIPT nakonfigurováno pro přidání nebo odebrání šifrování TLS. To znamená, že přenosová cesta MQIPT může být nakonfigurována s `SSLServer=true` a `SSLClient=false`nebo `SSLServer=true` a `SSLClient=false`. V této situaci se klientovi a správci front nemusí podařit dohodnout algoritmus ochrany hesla, protože jeden konec kanálu používá šifrování TLS a druhý nikoli. To způsobí selhání připojení s kódem příčiny MQRC_PASSWORD_PROTECTION_ERROR (2594).

V produktu IBM MQ 9.3.1může produkt MQIPT přidat nebo odebrat ochranu pro pověření ve strukturách MQCSP, aby byla zachována kompatibilita mezi klientem a správcem front pro trasy MQIPT , které přidávají nebo odebírají šifrování TLS. Ochrana heslem MQCSP v produktu MQIPT je konfigurována pomocí vlastnosti trasy **PasswordProtection** .

Výchozí hodnota vlastnosti **PasswordProtection** je `povinná`. Tato hodnota znamená, že produkt MQIPT je schopen přidat, ale ne odebrat, ochranu pomocí hesla MQCSP. Připojení k trase MQIPT , která přidává šifrování TLS, mohou selhat s kódem příčiny MQRC_PASSWORD_PROTECTION_ERROR (2594) s touto hodnotou **PasswordProtection**. Chcete-li vyřešit tento problém, nastavte hodnotu vlastnosti **PasswordProtection** na `kompatibilní` v konfiguraci trasy MQIPT .

Další informace o vlastnosti **PasswordProtection** v souboru MQIPTviz PasswordProtection.

Správce digitálních certifikátů (DCM)

Pomocí produktu DCM můžete spravovat digitální certifikáty a soukromé klíče v systému IBM i.

Produkt DCM (Digital Certificate Manager) vám umožňuje spravovat digitální certifikáty a používat je v zabezpečených aplikacích na serveru IBM i . Pomocí produktu Digital Certificate Managermůžete požadovat a zpracovávat digitální certifikáty od certifikačních autorit (CA) nebo jiných třetích stran. Můžete také vystupovat jako lokální certifikační autorita pro vytváření a správu digitálních certifikátů pro vaše uživatele.

Produkt DCM také podporuje používání seznamů odvolaných certifikátů (CRL), aby poskytoval silnější certifikát a proces ověřování aplikací. Pomocí produktu DCM můžete definovat umístění, kde se určitý seznam CRL certifikační autority nachází na serveru LDAP, aby mohl produkt IBM MQ ověřit, že určitý certifikát nebyl odvolán.

Produkt DCM podporuje a může automaticky detekovat certifikáty v různých formátech. Když produkt DCM zjistí certifikát kódovaný pomocí PKCS #12 nebo certifikát PKCS #7 , který obsahuje šifrovaná data, automaticky vyzve uživatele k zadání hesla, které bylo použito k zašifrování certifikátu. Produkt DCM nevyzve k certifikátům PKCS #7 , které neobsahují šifrovaná data.

Produkt DCM poskytuje uživatelské rozhraní založené na prohlížeči, které můžete použít ke správě digitálních certifikátů pro vaše aplikace a uživatele. Uživatelské rozhraní je rozděleno do dvou hlavních rámců: navigačního rámce a rámce úloh.

Navigační rámec se používá k výběru úloh pro správu certifikátů nebo aplikací, které je používají. Některé jednotlivé úlohy jsou zobrazeny přímo v hlavním navigačním rámci, ale většina úloh v navigačním rámci je uspořádána do kategorií. Například, Správa certifikátů je kategorie úloh, která obsahuje různé jednotlivé vedené úlohy, jako např. Zobrazit certifikát, Obnovit certifikát a Importovat certifikát. Pokud je položka v navigačním rámci kategorií, která obsahuje více než jednu úlohu, zobrazí se vlevo od ní šipka. Šipka označuje, že když vyberete odkaz na kategorii, zobrazí se rozbalený seznam úloh, který vám umožní vybrat, kterou úlohu provést.

Důležité informace o produktu DCM naleznete v následujících příručkách produktu IBM Redbooks :

- *IBM i Zabezpečení pevné sítě: OS/400 V5R1 DCM a šifrovací vylepšení*, SG24-6168. Základní informace o nastavení systému IBM i jako lokálního CA naleznete v apendixech.
- *AS/400 Internetová bezpečnost: Vývoj infrastruktury digitálního certifikátu*, SG24-5659. Konkrétně viz kapitola 5. *Digital Certificate Manager pro AS/400* , který vysvětluje produkt AS/400 DCM.

Federální standardy zpracování informací (FIPS)

Toto téma představuje program FIPS (Federal Information Processing Standards) Cryptomodule Validation Program Národního institutu pro standardy a technologie USA a šifrovací funkce, které lze použít na kanálech TLS.

Poznámka: V systému AIX, Linux, and Windowsposkytuje produkt IBM MQ kompatibilitu se standardem FIPS 140-2 prostřednictvím šifrovacího modulu IBM Crypto for C (ICC) . Certifikát pro tento modul byl přesunut do historického stavu. Zákazníci by si měli prohlédnout IBM Crypto for C (ICC) certifikát a měli by si být vědomi všech doporučení poskytnutých NIST. Náhradní modul FIPS 140-3 momentálně probíhá a jeho stav lze zobrazit jeho vyhledáním v modulech NIST CMVP v seznamu procesů.

Tyto informace se vztahují na následující platformy:

- ALW AIX, Linux, and Windows
- z/OS z/OS

ALW Další informace o shodě FIPS 140-2 IBM MQ připojení TLS v systému AIX, Linux, and Windowsviz “Standard FIPS (Federal Information Processing Standards) pro AIX, Linux, and Windows” na stránce 34.

z/OS Další informace o shodě FIPS 140-2 IBM MQ připojení TLS v systému z/OSviz “Standard FIPS (Federal Information Processing Standards) pro z/OS” na stránce 37.

Je-li přítomen kryptografický hardware, mohou být kryptografické moduly používané produktem IBM MQ konfigurovány tak, aby byly ty, které poskytuje výrobce hardwaru. Pokud se tak stane, je konfigurace kompatibilní pouze se standardem FIPS, pokud jsou tyto šifrovací moduly certifikovány FIPS.

V průběhu času jsou federální standardy zpracování informací aktualizovány tak, aby odrážely nové útoky proti šifrovacím algoritmům a protokolům. Například některé specifikace CipherSpecs mohou přestat být certifikovány FIPS. Dojde-li k takovým změnám, produkt IBM MQ se také aktualizuje, aby implementoval nejnovější standard. V důsledku toho může dojít po provedení údržby ke změnám chování.

Související pojmy

“Určení, že se za běhu v klientu MQI používají pouze specifikace CipherSpecs s certifikací FIPS.” na stránce 270
Vytvořte úložiště klíčů pomocí softwaru vyhovujícího standardu FIPS a poté určete, že kanál musí používat specifikace CipherSpecss certifikací FIPS.

“Použití příkazu runmqckm, runmqakm a strmqikm ke správě digitálních certifikátů” na stránce 293
V systémech AIX, Linux, and Windows spravujte klíče a digitální certifikáty pomocí konzoly **strmqikm** (iKeyman). Grafické rozhraní nebo z příkazového řádku pomocí **runmqckm** (iKeycmd) nebo **runmqakm** (GSKCapiCmd).

Související úlohy

Povolení TLS v produktu IBM MQ classes for Java

Použití protokolu TLS (Transport Layer Security) s produktem IBM MQ classes for JMS

Související odkazy

Vlastnosti TLS objektů JMS

“Federální standardy zpracování informací” na stránce 23
Americká vláda poskytuje technické poradenství v oblasti IT systémů a bezpečnosti, včetně šifrování dat. Národní institut pro normy a technologie (NIST) je důležitým orgánem, který se zabývá IT systémy a bezpečností. NIST vytváří doporučení a standardy, včetně standardů FIPS (Federal Information Processing Standards).

ALW *Standard FIPS (Federal Information Processing Standards) pro AIX, Linux, and Windows*
Je-li v systémech AIX, Linux, and Windows vyžadováno šifrování v kanálu SSL/TLS, používá produkt IBM MQ šifrovací balík s názvem IBM Crypto for C (ICC). Na platformách AIX, Linux, and Windows prošel software ICC programem FIPS (Federal Information Processing Standards) Cryptomodule Validation Program amerického Národního institutu pro standardy a technologie (US National Institute of Standards and Technology) na úrovni 140-2.

Poznámka: V systému AIX, Linux, and Windowsposkytuje produkt IBM MQ kompatibilitu se standardem FIPS 140-2 prostřednictvím šifrovacího modulu IBM Crypto for C (ICC) . Certifikát pro tento modul byl přesunut do historického stavu. Zákazníci by si měli prohlédnout IBM Crypto for C (ICC) certifikát a měli by si být vědomi všech doporučení poskytnutých NIST. Náhradní modul FIPS 140-3 momentálně probíhá a jeho stav lze zobrazit jeho vyhledáním v modulech NIST CMVP v seznamu procesů.

Shoda připojení IBM MQ TLS na systémech AIX, Linux, and Windows se standardem FIPS 140-2 je následující:

- Pro všechny kanály zpráv IBM MQ (s výjimkou typů kanálů CLNTCONN) je připojení kompatibilní se standardem FIPS, pokud jsou splněny následující podmínky:

  - Nainstalovaná verze produktu IBM Global Security Kit (GSKit) ICC byla certifikována podle standardu FIPS 140-2 na nainstalované verzi operačního systému a hardwarové architektuře.
  - Atribut SSLFIPS správce front byl nastaven na hodnotu YES.
  - Všechna úložiště klíčů byla vytvořena a byla s nimi manipulována pouze pomocí softwaru vyhovujícího standardu FIPS, například **runmqakm** s volbou `-fips` .
  - Přístup ke všem úložištím klíčů je poskytován pomocí souboru pro dočasné ukládání, nikoli pomocí atributu **KEYRPWD** správce front.
- Pro všechny aplikace IBM MQ MQI client připojení používá produkt GSKit a vyhovuje standardu FIPS, pokud jsou splněny následující podmínky:
  - Nainstalovaná verze produktu GSKit ICC byla certifikována podle standardu FIPS 140-2 na nainstalované verzi operačního systému a hardwarové architektuře.
  - Určili jste, že má být použito pouze šifrování s certifikací FIPS, jak je popsáno v souvisejícím tématu pro klienta MQI.
  - Všechna úložiště klíčů byla vytvořena a byla s nimi manipulována pouze pomocí softwaru vyhovujícího standardu FIPS, například **runmqakm** s volbou `-fips` .
  - Přístup ke všem úložištím klíčů je poskytován pomocí souboru pro dočasné ukládání, nikoli pomocí mechanizmu hesla úložiště klíčů.
- Pro aplikace IBM MQ classes for Java používající režim klienta používá připojení implementace TLS prostředí JRE a vyhovuje standardu FIPS, pokud jsou splněny následující podmínky:
  - Běhové prostředí Java použité ke spuštění aplikace vyhovuje standardu FIPS na nainstalované verzi operačního systému a architektuře hardwaru.
  - Určili jste, že se má použít pouze šifrování s certifikací FIPS, jak je popsáno v souvisejícím tématu pro klienta Java .
  - Všechna úložiště klíčů byla vytvořena a byla s nimi manipulována pouze pomocí softwaru vyhovujícího standardu FIPS, například **runmqakm** s volbou `-fips` .
- Pro aplikace IBM MQ classes for JMS používající režim klienta používá připojení implementace TLS prostředí JRE a vyhovuje standardu FIPS, pokud jsou splněny následující podmínky:
  - Běhové prostředí Java použité ke spuštění aplikace vyhovuje standardu FIPS na nainstalované verzi operačního systému a architektuře hardwaru.
  - Určili jste, že se má použít pouze šifrování s certifikací FIPS, jak je popsáno v souvisejícím tématu pro klienta JMS .
  - Všechna úložiště klíčů byla vytvořena a byla s nimi manipulována pouze pomocí softwaru vyhovujícího standardu FIPS, například **runmqakm** s volbou `-fips` .
- Pro nespravované klientské aplikace .NET používá připojení produkt GSKit a vyhovuje standardu FIPS, pokud jsou splněny následující podmínky:
  - Nainstalovaná verze produktu GSKit ICC byla certifikována podle standardu FIPS 140-2 na nainstalované verzi operačního systému a hardwarové architektuře.
  - Určili jste, že se má použít pouze šifrování s certifikací FIPS, jak je popsáno v souvisejícím tématu pro klienta .NET .
  - Všechna úložiště klíčů byla vytvořena a byla s nimi manipulována pouze pomocí softwaru vyhovujícího standardu FIPS, například **runmqakm** s volbou `-fips` .
  - Přístup ke všem úložištím klíčů je poskytován pomocí souboru pro dočasné ukládání, nikoli pomocí mechanizmu hesla úložiště klíčů.
- Pro nespravované klientské aplikace XMS .NET používá připojení produkt GSKit a vyhovuje standardu FIPS, pokud jsou splněny následující podmínky:
  - Nainstalovaná verze produktu GSKit ICC byla certifikována podle standardu FIPS 140-2 na nainstalované verzi operačního systému a hardwarové architektuře.
  - Uvedli jste, že se má použít pouze šifrování s certifikací FIPS, jak je popsáno v dokumentaci XMS .NET .

- Všechna úložiště klíčů byla vytvořena a byla s nimi manipulována pouze pomocí softwaru vyhovujícího standardu FIPS, například **runmqakm** s volbou `-fips` .
- Přístup ke všem úložištím klíčů je poskytován pomocí souboru pro dočasné ukládání, nikoli pomocí mechanizmu hesla úložiště klíčů.

Všechny podporované platformy mají certifikaci FIPS 140-2, s výjimkou toho, jak je uvedeno v souboru README, který je součástí každé opravné sady nebo aktualizační sady.

Pro připojení TLS používající produkt GSKitje komponenta, která je certifikována podle standardu FIPS 140-2, pojmenována *ICC*. Je to verze této komponenty, která určuje shodu se standardem GSKit FIPS na jakékoli dané platformě. Chcete-li určit aktuálně nainstalovanou verzi produktu ICC , spusťte příkaz **dspmqver -p 64 -v** .

Zde je příklad extrakce výstupu **dspmqver -p 64 -v** souvisejícího s produktem ICC:

```
Mezinárodní trestní soud
============
@ (#)CompanyName: IBM Corporation
@(#)LegalTrademarks: IBM
@ (#)FileDescription: IBM Crypto for C-language
@(#)FileVersion:   8.0.0.0
@ (#)LegalCopyright: Licencované materiály-vlastnictví IBM
@ (#) ICC
@ (#) (C) Copyright IBM Corp. 2002, 2024.
@ (#) Všechna práva vyhrazena. Uživatelé vlády USA
@ (#) Omezená práva-Použití, kopírování nebo zveřejnění
@ (#) omezeno smlouvou GSA ADP Schedule Contract se společností IBM Corp.
@ (#)ProductName: icc_8.0 (sestaveníGoldCoast ) 100415
@(#)ProductVersion:  8.0.0.0
@(#)ProductInfo:   10/04/15.03:32:19.10/04/15.18:41:51
@ (#) CMVCInfo:
```

Prohlášení o certifikaci NIST pro GSKit ICC 8 (obsaženo v GSKit 8) lze nalézt na následující adrese: Cryptographic Module Validation Program.

Je-li přítomen kryptografický hardware, mohou být kryptografické moduly používané produktem IBM MQ konfigurovány tak, aby byly ty, které poskytuje výrobce hardwaru. Pokud se tak stane, je konfigurace kompatibilní pouze se standardem FIPS, pokud jsou tyto šifrovací moduly certifikovány FIPS.

Vynucená omezení Triple DES při provozu v souladu se standardem FIPS 140-2

Je-li produkt IBM MQ konfigurován tak, aby pracoval v souladu se standardem FIPS 140-2, jsou vynucena další omezení v souvislosti se specifikací Triple DES (3DES) CipherSpecs. Tato omezení umožňují shodu s doporučením US NIST SP800-67 .

1. Všechny části klíče Triple DES musí být jedinečné.
2. Žádná část klíče Triple DES nemůže být slabá, částečně slabá nebo možná slabá podle definic v NIST SP800-67.
3. Před resetem tajného klíče nelze přes připojení přenést více než 32 GB dat. Standardně produkt IBM MQ nevynuluje tajný klíč relace, takže tento reset musí být nakonfigurován. Selhání při povolení resetu tajného klíče při použití specifikace Triple DES CipherSpec a shody FIPS 140-2 má za následek zavření připojení s chybou AMQ9288 po překročení maximálního počtu bajtů. Chcete-li získat informace o tom, jak nakonfigurovat reset tajného klíče, prohlédněte si téma “Resetování tajných klíčů SSL a TLS” na stránce 483.

Produkt IBM MQ generuje klíče relace Triple DES, které již vyhovují pravidlům 1 a 2. Chcete-li však splnit třetí omezení, musíte povolit reset tajného klíče při použití specifikací Triple DES CipherSpecs v konfiguraci FIPS 140-2. Alternativně se můžete vyhnout použití Triple DES.

Související pojmy

“Určení, že se za běhu v klientu MQI používají pouze specifikace CipherSpecs s certifikací FIPS.” na stránce 270
Vytvořte úložiště klíčů pomocí softwaru vyhovujícího standardu FIPS a poté určete, že kanál musí používat specifikace CipherSpecss certifikací FIPS.

“Použití příkazu runmqckm, runmqakm a strmqikm ke správě digitálních certifikátů” na stránce 293

V systémech AIX, Linux, and Windows spravujte klíče a digitální certifikáty pomocí konzoly **strmqikm** (iKeyman). Grafické rozhraní nebo z příkazového řádku pomocí **runmqckm** (iKeycmd) nebo **runmqakm** (GSKCapiCmd).

Související úlohy

Povolení TLS v produktu IBM MQ classes for Java

Použití protokolu TLS (Transport Layer Security) s produktem IBM MQ classes for JMS

Související odkazy

Vlastnosti TLS objektů JMS

“Federální standardy zpracování informací” na stránce 23

Americká vláda poskytuje technické poradenství v oblasti IT systémů a bezpečnosti, včetně šifrování dat. Národní institut pro normy a technologie (NIST) je důležitým orgánem, který se zabývá IT systémy a bezpečností. NIST vytváří doporučení a standardy, včetně standardů FIPS (Federal Information Processing Standards).

z/OS *Standard FIPS (Federal Information Processing Standards) pro z/OS*

Je-li v kanálu SSL/TLS v systému z/OS vyžadováno šifrování, produkt IBM MQ používá službu s názvem System SSL. Cílem zabezpečení SSL systému je poskytnout schopnost zabezpečeného provádění v režimu, který je navržen tak, aby dodržoval program FIPS (Federal Information Processing Standards) Cryptomodule Validation Program amerického Národního institutu pro standardy a technologie na úrovni 140-2.

Při implementaci připojení kompatibilních se standardem FIPS 140-2 s připojeními TLS produktu IBM MQ je třeba zvážit několik bodů:

- Chcete-li povolit kanály zpráv IBM MQ pro shodu s FIPS, ujistěte se, že jsou splněny následující podmínky:
  - Je nainstalováno a nakonfigurováno FMID zabezpečení SSL systému úrovně 3 (viz Plánování instalace IBM MQ).
  - Moduly SSL systému jsou ověřeny.
  - Atribut SSLFIPS správce front byl nastaven na hodnotu **YES**.

Při provádění v režimu FIPS systémové zabezpečení SSL využívá funkci CPACF (CP Assist for Cryptographic Function), je-li k dispozici. Šifrovací funkce prováděné hardwarem podporovaným ICSF při spuštění v režimu jiném než FIPS jsou nadále využívány při provádění v režimu FIPS, s výjimkou generování podpisu RSA, které musí být provedeno v softwaru.

Tabulka 2. Rozdíly mezi režimem FIPS a podporou algoritmu jiného režimu než FIPS.

	Jiné než FIPS		**FIPS**	
algoritmus	**Velikosti klíčů**	**Hardware**	**Velikosti klíčů**	**Hardware**
RC2	40 a 128			
RC4	40 a 128			
DES	56	x		
TDES	168	x	168	x
AES	128 a 256	x	128 a 256	x
MD5	48			
SHA-1	160	x	160	x
SHA-2	224, 256, 384 a 512	x	224, 256, 384 a 512	x
RSA	512-4096	x	1024-4096	x

Tabulka 2. Rozdíly mezi režimem FIPS a podporou algoritmu jiného režimu než FIPS. (pokračování)				
	Jiné než FIPS		**FIPS**	
algoritmus	**Velikosti klíčů**	**Hardware**	**Velikosti klíčů**	**Hardware**
DSA	512-1024 (počet)		1024	
DH	512-2048		2048	

V režimu FIPS může systémové zabezpečení SSL používat pouze certifikáty, které používají algoritmy a velikosti klíčů uvedené v tabulce 1. Je-li během ověřování certifikátu X.509 zjištěn algoritmus, který je nekompatibilní s režimem FIPS, nelze certifikát použít a je s ním zacházeno jako s neplatným.

Informace o aplikacích tříd IBM MQ používajících režim klienta v rámci produktu WebSphere Application Server naleznete v tématu Podpora standardu zpracování federálních informací.

Informace o konfiguraci modulu SSL systému naleznete v tématu Nastavení ověření modulu SSL systému .

Související odkazy

“Federální standardy zpracování informací” na stránce 23
Americká vláda poskytuje technické poradenství v oblasti IT systémů a bezpečnosti, včetně šifrování dat. Národní institut pro normy a technologie (NIST) je důležitým orgánem, který se zabývá IT systémy a bezpečností. NIST vytváří doporučení a standardy, včetně standardů FIPS (Federal Information Processing Standards).

Multi

Ověření konfigurace TLS vašeho správce front pomocí `mqcertck`

Příkaz **MQCERTCK** je nástroj pro vyhledání běžných chyb v konfiguraci TLS vašeho správce front a poskytuje některé návrhy pro řešení problémů.

Úvod

Příkaz **`mqcertck`** zkontroluje:

- Existence a oprávnění úložiště klíčů správce front, na které odkazuje atribut **SSLKEYR** správce front.
- Existence a platnost certifikátu pro certifikát správce front, na který odkazuje atribut **CERTLABL** správce front.
- Existence a platnost všech certifikátů odkazovaných v atributech **CERTLABL** kanálu s povoleným zabezpečením TLS.
- Úložiště klíčů a certifikáty klientských aplikací, včetně kontroly certifikátů, jsou autorizovány se správcem front.

Poznámka: Příkaz **`mqcertck`** není v systému z/OS nebo IBM ik dispozici.

Pouľití

Chcete-li použít příkaz **`mqcertck`** , spusťte příkaz `mqcertck`spolu s jeho požadovanými parametry a všemi požadovanými volitelnými parametry z příkazového řádku.

Popis příkazu a parametrů, které příkaz přijímá, viz mqcertck .

Příklad

Právě jste dokončili nastavení správce front `QM1` tak, aby umožňoval připojení TLS z klientů, kteří se připojují ke kanálu SVRCONN vašeho správce front.

Používáte funkci více certifikátů, takže jak správce front, tak i kanál mají popisek certifikátu uvedený v jejich atributech **CERTLABL** . Při vytváření kanálu jste udělali chybu v atributu **CERTLABL** kanálu, takže když se klient pokusí připojit, vrátí správce front návratový kód 2393 MQRC_SSL_INITIALIZATION_ERROR.

Před aktivací správce front použijte příkaz **mqcertck** k ověření konfigurace TLS správce front.

Spustíte příkaz `mqcertck QM1` a obdržíte následující výstup:

```
5724-H72 (C) Copyright IBM Corp. 1994, 2024.
+-----------------------------------------------------------
| IBM MQ TLS Configuration Test tool
+-----------------------------------------------------------
| Problem identified:
|  No certificate could be found for the channel
|  MQCERTCK.CHANNEL
|  This tool looked in the Queue Manager's key repository
|  located at: 'C:\MQ Data\qmgrs\QM1\ssl\key.kdb'
|  for a certificate with label 'chacert',
|  which is the certificate specified in the channel's
|  CERTLABL attribute, but was unable to find one.
|
| Possible resolution:
|  A valid certificate with the label chacert
|  needs to be added to the key repository.
|
|  Alternatively, alter the channel definition to remove
|  the CERTLABL value. This can be done by executing the
|  following command in runmqsc:
|      ALTER CHANNEL(<Name>) CHLTYPE(<TYPE>) CERTLABL(' ')
+-----------------------------------------------------------
| mqcertck has ended. See above for any problems found.
| If there are problems then resolve these and run this
| tool again.
|
+-----------------------------------------------------------
```

Tento výstup vás vyzve ke kontrole definice kanálu pro kanál připojení serveru MQCERTCK.CHANNEL. Zde uvidíte chybu, kterou jste provedli, a můžete ji opravit před opětovným spuštěním příkazu `mqcertck` , abyste ověřili, že jste problém vyřešili.

Ověření připojení klienta

Příkaz **mqcertck** má schopnost ověřit úložiště klíčů klienta a konfiguraci TLS správce front. K tomu je třeba, aby produkt **mqcertck** měl přístup k úložišti klíčů klienta z počítače, na kterém je spuštěn správce front.

Pokud při spuštění příkazu **mqcertck** zadáte parametr **-clientkeyr** s umístěním úložiště klíčů klienta (bez rozšíření) **mqcertck** , zkontroluje toto úložiště klíčů ve vztahu ke správci front.

Pokud víte, který kanál bude klient používat pro připojení ke správci front, můžete jej zadat pomocí příznaku **-clientchannel** .

Pokud klient používá vzájemné ověření pro připojení ke správci front, můžete použít parametr **-clientusername** nebo **-clientlabel** a sdělit příkazu **mqcertck** , který certifikát má být použit v úložišti klíčů klienta.

Pokud používáte výchozí certifikát a nezadáváte popisek certifikátu klientské aplikaci, můžete použít parametry **-clientusername** a **username** , které spouští tuto aplikaci.

Během operace příkazu **mqcertck** příkaz vygeneruje popisek certifikátu `ibmwebspheremqXXXX` , kde XXXX je hodnota předaná v parametru **-clientusername** .

Chcete-li plně ověřit úložiště klíčů klienta, příkaz **mqcertck** vytvoří fiktivní připojení pomocí IBM Global Security Kit (GSKit). Chcete-li to provést, musí mít příkaz k dispozici port, ke kterému se může připojit během testů klienta. Výchozí použitý port je 5857, avšak pokud se již používá, můžete uvést jiný port, který se má použít během testů klienta.

Poznámka: Ačkoli se příkaz **mqcertck** váže na port, produkt **mqcertck**nepoužívá žádnou externí komunikaci a všechny testy se provádějí lokálně.

SSL/TLS na serveru IBM MQ MQI client

Produkt IBM MQ podporuje protokol TLS v klientech. Použití TLS můžete upravit různými způsoby.

Produkt IBM MQ poskytuje podporu TLS pro IBM MQ MQI clients na systémech AIX, Linux, and Windows . Pokud používáte produkt IBM MQ classes for Java, prohlédněte si téma Použití produktu IBM MQ classes for Java a pokud používáte produkt IBM MQ classes for JMS, prohlédněte si téma Použití produktu IBM MQ classes for JMS. Zbytek tohoto oddílu se nevztahuje na prostředí Java nebo JMS .

Úložiště klíčů pro položku IBM MQ MQI client můžete zadat buď s hodnotou MQSSLKEYR v konfiguračním souboru klienta IBM MQ , nebo při volání MQCONNX aplikací. Máte tři možnosti, jak určit, že kanál používá protokol TLS:

- Použití tabulky definic kanálů
- Použití struktury voleb konfigurace SSL MQSCO ve volání MQCONNX
- Použití Active Directory (na systémech Windows)

Pomocí proměnné prostředí MQSERVER nelze určit, že kanál používá protokol TLS.

Můžete pokračovat ve spouštění existujících aplikací IBM MQ MQI client bez TLS, pokud není TLS uvedeno na druhém konci kanálu.

Pokud jsou v klientském počítači provedeny změny obsahu úložiště klíčů TLS, umístění úložiště klíčů TLS, ověřovacích informací nebo parametrů šifrovacího hardwaru, musíte ukončit všechna připojení TLS, aby se tyto změny projevily v kanálech připojení klienta, které aplikace používá pro připojení ke správci front. Po ukončení všech připojení restartujte kanály TLS. Použijí se všechna nová nastavení TLS. Tato nastavení jsou obdobná nastavením aktualizovaným příkazem REFRESH SECURITY TYPE (SSL) v systémech správce front.

Když je produkt IBM MQ MQI client spuštěn na systému AIX, Linux, and Windows s šifrovacím hardwarem, konfigurujte tento hardware pomocí proměnné prostředí MQSSLCRYP. Tato proměnná je ekvivalentní parametru SSLCRYP v příkazu ALTER QMGR MQSC. Popis parametru SSLCRYP v příkazu ALTER QMGR MQSC viz ALTER QMGR . Používáte-li verzi GSK_PCS11 parametru SSLCRYP, musí být popisek tokenu PKCS #11 uveden zcela malými písmeny.

Obnovení tajného klíče TLS a FIPS jsou podporovány na systému IBM MQ MQI clients. Další informace naleznete v tématech “Resetování tajných klíčů SSL a TLS” na stránce 483 a “Standard FIPS (Federal Information Processing Standards) pro AIX, Linux, and Windows” na stránce 34.

Další informace o podpoře TLS pro produkt IBM MQ MQI clientsnaleznete v tématu “Nastavení zabezpečení IBM MQ MQI client” na stránce 269 .

Související úlohy

IBM MQ MQI client konfigurační soubor, `mqclient.ini`

Určení, že kanál MQI používá SSL/TLS

Má-li kanál MQI používat protokol TLS, musí být hodnotou atributu *SSLCipherSpec* kanálu připojení klienta název CipherSpec podporované produktem IBM MQ na platformě klienta.

Kanál připojení klienta s hodnotou tohoto atributu můžete definovat následujícími způsoby. Jsou uvedeny v pořadí podle klesající priority.

1. Když uživatelská procedura PreConnect poskytuje strukturu definice kanálu, která se má použít.

   Uživatelská procedura PreConnect může poskytnout název CipherSpec v poli *SSLCipherSpec* struktury definice kanálu MQCD. Tato struktura je vrácena v poli **ppMQCDArrayPtr** struktury parametrů uživatelské procedury MQNXP používané uživatelskou procedurou PreConnect .

2. Když aplikace IBM MQ MQI client vydá volání MQCONNX.

   Aplikace může zadat název CipherSpec v poli *SSLCipherSpec* struktury definice kanálu MQCD.Na tuto strukturu odkazuje struktura voleb připojení MQCNO, která je parametrem volání MQCONNX.

3. Použití tabulky CCDT (Client Channel Definition Table).

   Jedna nebo více položek v tabulce definic kanálů klienta může určovat název CipherSpec.Pokud například vytvoříte položku pomocí příkazu DEFINE CHANNEL MQSC, můžete pomocí parametru SSLCIPH v příkazu zadat název CipherSpec.

4. Použití Active Directory v systému Windows.

Na systémech Windows můžete použít řídicí příkaz **setmqscp** k publikování definic kanálů připojení klienta v adresáři Active Directory. Jedna nebo více těchto definic může určovat název CipherSpec.

Pokud například aplikace klienta poskytuje definici kanálu připojení klienta ve struktuře MQCD ve volání MQCONNX, bude tato definice použita namísto položek v tabulce definic kanálů klienta, k nimž má klient IBM MQ přístup.

Proměnnou prostředí MQSERVER nelze použít k zadání definice kanálu na konci klienta kanálu MQI, který používá protokol TLS.

Chcete-li zkontrolovat, zda došlo k toku certifikátu klienta, zobrazte stav kanálu na konci serveru kanálu pro přítomnost hodnoty parametru názvu typu peer.

Související pojmy

"Určení CipherSpec pro IBM MQ MQI client" na stránce 461
Máte tři volby pro určení CipherSpec pro IBM MQ MQI client.

CipherSpecs a CipherSuites v souboru IBM MQ

Produkt IBM MQ podporuje protokoly TLS1.3 a TLS 1.2 CipherSpecsa algoritmy RSA a Diffie-Hellman. V případě potřeby však můžete povolit zamítnuté specifikace CipherSpecs.

See "Povolení CipherSpecs" na stránce 438 for information on:

- CipherSpecs podporované produktem IBM MQ.
- Jak povolíte zamítnuté specifikace SSL 3.0 a TLS 1.0 CipherSpecs.

Produkt IBM MQ podporuje algoritmy pro výměnu klíčů a ověřování RSA a Diffie-Hellman. Velikost klíče použitého během navázání komunikace TLS může záviset na použitém digitálním certifikátu, ale některé specifikace CipherSpecs obsahují specifikaci velikosti klíče navázání komunikace. Větší klíče pro navázání komunikace poskytují silnější ověření. Vyjednávání v případě menších klíčů je rychlejší.

Související pojmy

"CipherSpecs a CipherSuites" na stránce 21
Šifrovací bezpečnostní protokoly se musí dohodnout na algoritmech používaných zabezpečeným připojením. CipherSpecs a CipherSuites definují specifické kombinace algoritmů.

Šifrování NSA Suite B v IBM MQ

Toto téma poskytuje informace o tom, jak nakonfigurovat produkt IBM MQ for AIX, Linux, and Windows tak, aby odpovídal profilu TLS 1.2 vyhovujícímu standardu Suite B.

V průběhu času je NSA Cryptography Suite B Standard aktualizován tak, aby odrážel nové útoky proti šifrovacím algoritmům a protokolům. Některé specifikace CipherSpecs mohou například přestat být certifikovány pro sadu Suite B. Dojde-li k takovým změnám, produkt IBM MQ se také aktualizuje, aby implementoval nejnovější standard. V důsledku toho může dojít po provedení údržby ke změnám chování. Soubor README IBM MQ uvádí verzi sady Suite B vynucenou každou úrovní údržby produktu. Pokud nakonfigurujete produkt IBM MQ tak, aby vynucoval shodu se sadou Suite B, vždy se při plánování použití údržby podívejte do souboru README. Viz téma IBM MQ, WebSphere MQ, a MQSeries product readmes.

Na systémech AIX, Linux, and Windows lze produkt IBM MQ nakonfigurovat tak, aby odpovídal profilu TLS vyhovujícímu standardu Suite B 1.2 na úrovních zabezpečení uvedených v tabulce 1.

Tabulka 3. Úrovně zabezpečení Suite B s povolenými specifikacemi CipherSpecs a algoritmy digitálního podpisu

Úroveň zabezpečení	**Povolené CipherSpecs**	**Povolené algoritmy digitálního podpisu**
128bitový	ECDHE_ECDSA_AES_128_GCM_SHA256 ECDHE_ECDSA_AES_256_GCM_SHA384	ECDSA s SHA-256 ECDSA s SHA-384
192bitový	ECDHE_ECDSA_AES_256_GCM_SHA384	ECDSA s SHA-384

Tabulka 3. Úrovně zabezpečení Suite B s povolenými specifikacemi CipherSpecs a algoritmy digitálního podpisu (pokračování)		
Úroveň zabezpečení	**Povolené CipherSpecs**	**Povolené algoritmy digitálního podpisu**
Obojí [1]	ECDHE_ECDSA_AES_128_GCM_SHA256 ECDHE_ECDSA_AES_256_GCM_SHA384	ECDSA s SHA-256 ECDSA s SHA-384

1. Současně je možné konfigurovat úrovně zabezpečení 128-bit i 192-bit. Vzhledem k tomu, že konfigurace sady Suite B určuje minimální přijatelné šifrovací algoritmy, je konfigurace obou úrovní zabezpečení ekvivalentní konfiguraci pouze 128bitové úrovně zabezpečení. Šifrovací algoritmy 192bitové úrovně zabezpečení jsou silnější než minimum požadované pro 128bitovou úroveň zabezpečení, takže jsou povoleny pro 128bitovou úroveň zabezpečení i v případě, že 192bitová úroveň zabezpečení není povolena.

Poznámka: Konvence pojmenování použité pro úroveň zabezpečení nemusí nutně představovat velikost eliptické křivky nebo velikost klíče šifrovacího algoritmu AES.

CipherSpec pro sadu B

Ačkoli výchozí chování produktu IBM MQ není v souladu se standardem Suite B, produkt IBM MQ lze nakonfigurovat tak, aby vyhovoval jedné nebo oběma úrovním zabezpečení na systémech AIX, Linux, and Windows . Po úspěšné konfiguraci produktu IBM MQ pro použití sady Suite B bude jakýkoli pokus o spuštění odchozího kanálu s použitím CipherSpec , která neodpovídá sadě Suite B, mít za následek chybu AMQ9282. Tato aktivita také způsobí, že klient MQI vrátí kód příčiny MQRC_CIPHER_SPEC_NOT_SUITE_B. Podobně pokus o spuštění příchozího kanálu s použitím CipherSpec neodpovídající konfiguraci Suite B vede k chybě AMQ9616.

Další informace o specifikacích IBM MQ CipherSpecsviz “Povolení CipherSpecs” na stránce 438

Sada B a digitální certifikáty

Sada B omezuje algoritmy digitálního podpisu, které lze použít k podepisování digitálních certifikátů. Sada B také omezuje typ veřejného klíče, který mohou certifikáty obsahovat. Proto musí být produkt IBM MQ nakonfigurován tak, aby používal certifikáty, jejichž algoritmus digitálního podpisu a typ veřejného klíče jsou povoleny nakonfigurovanou úrovní zabezpečení Suite B vzdáleného partnera. Digitální certifikáty, které nesplňují požadavky na úroveň zabezpečení, jsou odmítnuty a připojení se nezdaří s chybou AMQ9633 nebo AMQ9285.

Pro 128bitovou úroveň zabezpečení Suite B je veřejný klíč subjektu certifikátu vyžadován pro použití eliptické křivky NIST P-256 nebo eliptické křivky NIST P-384 a pro podepsání eliptické křivky NIST P-256 nebo eliptické křivky NIST P-384 . Na úrovni zabezpečení 192bitové sady B je veřejný klíč předmětu certifikátu vyžadován pro použití eliptické křivky NIST P-384 a pro podepsání eliptickou křivkou NIST P-384 .

Chcete-li získat certifikát vhodný pro operaci vyhovující standardu Suite B, použijte příkaz **runmqakm** a zadejte parametr **-sig_alg** pro vyžádání vhodného algoritmu digitálního podpisu. Hodnoty parametrů EC_ecdsa_with_SHA256 a EC_ecdsa_with_SHA384 **-sig_alg** odpovídají klíčům eliptické křivky podepsaným povolenými algoritmy digitálního podpisu Suite B.

Další informace o příkazu **runmqakm** viz volby runmqckm a runmqakm.

Poznámka: Příkazy **runmqckm** a **strmqikm** nepodporují vytváření digitálních certifikátů pro operace vyhovující standardu Suite B.

Vytvoření a vyžádání digitálních certifikátů

Chcete-li vytvořit digitální certifikát podepsaný svým držitelem pro testování sady Suite B, viz “Vytvoření osobního certifikátu podepsaného (svým) držitelem v systému AIX, Linux, and Windows” na stránce 308

Chcete-li požádat o digitální certifikát podepsaný certifikační autoritou pro produkční použití sady Suite B, viz “Vyžádání osobního certifikátu na AIX, Linux, and Windows” na stránce 310.

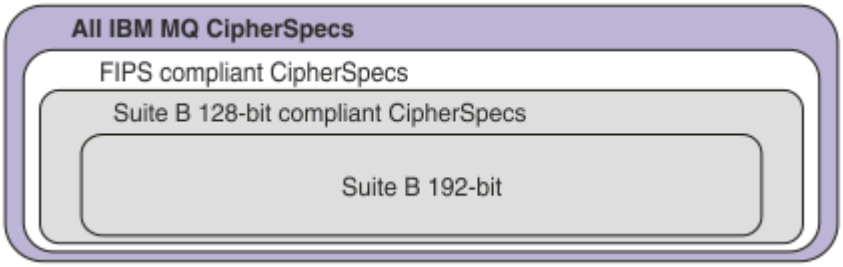
Poznámka: Používaná certifikační autorita musí generovat digitální certifikáty, které splňují požadavky popsané v IETF RFC 6460.

FIPS 140-2 a Suite B

Poznámka: V systému AIX, Linux, and Windowsposkytuje produkt IBM MQ kompatibilitu se standardem FIPS 140-2 prostřednictvím šifrovacího modulu IBM Crypto for C (ICC) . Certifikát pro tento modul byl přesunut do historického stavu. Zákazníci by si měli prohlédnout IBM Crypto for C (ICC) certifikát a měli by si být vědomi všech doporučení poskytnutých NIST. Náhradní modul FIPS 140-3 momentálně probíhá a jeho stav lze zobrazit jeho vyhledáním v modulech NIST CMVP v seznamu procesů.

Standard Suite B je koncepčně podobný standardu FIPS 140-2, protože omezuje sadu povolených šifrovacích algoritmů, aby poskytoval zajištěnou úroveň zabezpečení. Momentálně podporované CipherSpecs sady Suite B lze použít, když je produkt IBM MQ nakonfigurován pro operaci vyhovující standardu FIPS 140-2. Proto je možné konfigurovat produkt IBM MQ pro shodu se standardem FIPS i sadou B současně. V takovém případě platí obě sady omezení.

Následující diagram ilustruje vztah mezi těmito dílčími sadami:



Konfigurace produktu IBM MQ pro operaci kompatibilní se sadou Suite B

Chcete-li získat informace o tom, jak nakonfigurovat IBM MQ na systému AIX, Linux, and Windows pro operaci vyhovující standardu Suite B, prohlédněte si téma “Konfigurace produktu IBM MQ pro sadu B” na stránce 43.

Produkt IBM MQ nepodporuje operaci kompatibilní se sadou Suite B na platformách IBM i a z/OS . Klienti IBM MQ Java a JMS také nepodporují operaci vyhovující standardu Suite B.

Související pojmy

“Určení, že se za běhu v klientu MQI používají pouze specifikace CipherSpecs s certifikací FIPS.” na stránce 270
Vytvořte úložiště klíčů pomocí softwaru vyhovujícího standardu FIPS a poté určete, že kanál musí používat specifikace CipherSpecss certifikací FIPS.

ALW *Konfigurace produktu IBM MQ pro sadu B*

Produkt IBM MQ lze nakonfigurovat tak, aby fungoval v souladu se standardem NSA Suite B na platformách AIX, Linux, and Windows .

Sada B omezuje sadu povolených šifrovacích algoritmů, aby poskytovala zajištěnou úroveň zabezpečení. Produkt IBM MQ lze nakonfigurovat tak, aby fungoval v souladu se sadou Suite B a poskytoval rozšířenou úroveň zabezpečení. Další informace o apartmá B viz “Národní bezpečnostní agentura (NSA) Suite B kryptografie” na stránce 23. Další informace o konfiguraci Suite B a jejím vlivu na kanály TLS naleznete v části “Šifrování NSA Suite B v IBM MQ” na stránce 41.

Správce front

Pro správce front použijte příkaz **ALTER QMGR** s parametrem **SUITEB** k nastavení hodnot odpovídajících požadované úrovni zabezpečení. Další informace viz ALTER QMGR.

Můžete také použít příkaz PCF **MQCMD_CHANGE_Q_MGR** s parametrem **MQIA_SUITE_B_STRENGTH** ke konfiguraci správce front pro operaci vyhovující standardu Suite B.

Poznámka: Pokud změníte nastavení sady B správce front, musíte restartovat službu MQXR, aby se tato nastavení projevila.

Klient MQI

Standardně klienti MQI nevynucují shodu sady Suite B. Můžete povolit klienta MQI pro shodu sady B provedením jedné z následujících voleb:

1. Nastavením pole EncryptionPolicySuiteB ve struktuře MQSCO ve volání MQCONNX na jednu nebo více z následujících hodnot:
   - `MQ_SUITE_B_NONE`
   - `MQ_SUITE_B_128_BIT`
   - `MQ_SUITE_B_192_BIT`

   Použití `MQ_SUITE_B_NONE` s jakoukoli jinou hodnotou je neplatné.

   Další informace o struktuře MQSCO naleznete v tématu Volby konfigurace MQSCO-SSL.
2. Nastavením proměnné prostředí **MQSUITEB** na jednu nebo více následujících hodnot:
   - `NONE`
   - `128_BIT`
   - `192_BIT`

   Můžete zadat více hodnot pomocí seznamu odděleného čárkami. Použití hodnoty `NONE` s jakoukoli jinou hodnotou je neplatné.
3. Nastavením atributu **EncryptionPolicySuiteB** v sekci SSL konfiguračního souboru klienta na jednu nebo více z následujících hodnot:
   - `NONE`
   - `128_BIT`
   - `192_BIT`

   Můžete zadat více hodnot pomocí seznamu odděleného čárkami. Použití `NONE` s jakoukoli jinou hodnotou je neplatné.

Poznámka: Nastavení klienta MQI jsou uvedena v pořadí podle priority. Struktura MSCO ve volání MQCONNX přepíše nastavení v proměnné prostředí **MQSUITEB** , které přepíše atribut v sekci SSL.

.NET

U .NET nespravovaných klientů vlastnost **MQC.ENCRYPTION_POLICY_SUITE_B** označuje požadovaný typ zabezpečení Suite B.

Informace o použití sady B v adresáři IBM MQ classes for .NETnaleznete v tématu Třída prostředí MQEnvironment .NET.

AMQP

Nastavení atributu Suite B pro správce front platí pro kanály AMQP v daném správci front. Pokud upravíte nastavení sady B správce front, musíte restartovat službu AMQP, aby se změny projevily.

Zásady ověřování certifikátů v adresáři IBM MQ

Zásada ověření platnosti certifikátu určuje, jak striktně je ověřování řetězu certifikátů v souladu s odvětvovým standardem zabezpečení.

Zásada ověření platnosti certifikátu závisí na platformě a prostředí takto:

- U aplikací Java a JMS na všech platformách závisí zásada ověření platnosti certifikátu na komponentě JSSE běhového prostředí Java . Další informace o zásadách ověřování certifikátů naleznete v dokumentaci k prostředí JRE.
- ALW Pro systémy AIX, Linux, and Windows je zásada ověření platnosti certifikátu dodána produktem IBM Global Security Kit (GSKit) a lze ji konfigurovat. Jsou podporovány dvě různé zásady ověřování certifikátů:
  - Starší zásada ověřování certifikátů, která se používá pro maximální zpětnou kompatibilitu a interoperabilitu se starými digitálními certifikáty, které nejsou v souladu s aktuálními normami pro ověřování platnosti certifikátů IETF. Tato zásada se nazývá Základní zásada.
  - Přísná zásada ověřování certifikátů vyhovující standardům, která vynucuje standard RFC 5280. Tato zásada je známa jako standardní zásada.
- IBM i Pro systémy IBM i závisí zásada ověření certifikátu na knihovně zabezpečených soketů poskytované operačním systémem. Další informace o zásadách ověřování certifikátů naleznete v dokumentaci k operačnímu systému.
- z/OS U systémů z/OS závisí zásada ověření certifikátu na komponentě System SSL, kterou poskytuje operační systém. Další informace o zásadách ověřování certifikátů naleznete v dokumentaci k operačnímu systému.

Chcete-li získat informace o tom, jak nakonfigurovat zásadu ověření platnosti certifikátu, prohlédněte si téma "Konfigurace zásad ověřování certifikátů v adresáři IBM MQ" na stránce 45. Další informace o rozdílech mezi základními a standardními zásadami ověřování certifikátů naleznete v tématu Ověření platnosti certifikátu a návrh zásad důvěryhodnosti na webu AIX, Linux, and Windows.

Konfigurace zásad ověřování certifikátů v adresáři IBM MQ

Existuje několik různých způsobů, jak určit, která zásada ověření certifikátu TLS se použije k ověření digitálních certifikátů přijatých ze vzdálených partnerských systémů.

Informace o této úloze

Zásada ověření platnosti certifikátu určuje, jak striktně je ověřování řetězu certifikátů v souladu s odvětvovým standardem zabezpečení. Zásada ověření platnosti certifikátu závisí na platformě a prostředí. Další informace o zásadách ověřování certifikátů naleznete v tématu "Zásady ověřování certifikátů v adresáři IBM MQ" na stránce 44.

Procedura

- Chcete-li nastavit zásadu ověřování certifikátů ve správci front, použijte atribut správce front **CERTVPOL**.

  Další informace o nastavení tohoto atributu naleznete v tématu ALTER QMGR (změna nastavení správce front).
- Chcete-li nastavit zásadu ověření platnosti certifikátu na klientovi, použijte následující metody.

  Pokud je k nastavení zásady použita více než jedna metoda, klient použije nastavení v následujícím pořadí priorit:

  1. Použijte pole `CertificateValPolicy` ve struktuře MQSCO klienta. Nastavte pole na jednu z následujících hodnot:

     MQ_CERT_VAL_POLICY_ANY
     Použijte všechny zásady ověřování certifikátů podporované knihovnou zabezpečených soketů. Přijměte řetěz certifikátů, pokud některá ze zásad považuje řetěz certifikátů za platný.

     MQ_CERT_VAL_POLICY_RFC5280
     Použijte pouze zásadu ověření certifikátu kompatibilní s produktem RFC5280 . Toto nastavení poskytuje přísnější ověření než nastavení ANY, ale odmítá některé starší digitální certifikáty.

     Další informace o použití tohoto pole naleznete v tématu Volby konfigurace MQSCO-SSL.

2. Použijte proměnnou prostředí klienta **MQCERTVPOL**. Chcete-li nastavit tuto proměnnou prostředí, použijte jeden z následujících příkazů:
   - Linux AIX Pro systémy AIX and Linux :

     ```
     export MQCERTVPOL= value
     ```

   - Windows Pro systémy Windows :

     ```
     SET MQCERTVPOL= value
     ```

   - IBM i Pro systémy IBM i :

     ```
     ADDENVVAR ENVVAR(MQCERTVPOL) VALUE(value)
     ```

3. Použijte atribut **CertificateValPolicy** sekce SSL v konfiguračním souboru klienta. Nastavte tento atribut na jednu z následujících hodnot:

   ANY
   Použijte všechny zásady ověřování certifikátů podporované základní knihovnou zabezpečených soketů. Toto nastavení je výchozí.

   RFC5280
   Použijte pouze ověření platnosti certifikátu, které je v souladu se standardem RFC 5280.

   Další informace o použití tohoto atributu naleznete v části Sekce SSL konfiguračního souboru klienta.

Digitální certifikáty a kompatibilita CipherSpec v produktu IBM MQ

Toto téma poskytuje informace o tom, jak zvolit příslušné specifikace CipherSpecs a digitální certifikáty pro vaši zásadu zabezpečení, a to nastíněním vztahu mezi specifikacemi CipherSpecs a digitálními certifikáty v produktu IBM MQ.

Se všemi podporovanými typy digitálních certifikátů lze použít pouze podmnožinu podporovaných specifikací CipherSpecs . Proto je nutné zvolit vhodnou specifikaci CipherSpec pro váš digitální certifikát. Podobně, pokud zásada zabezpečení vaší organizace vyžaduje, abyste použili konkrétní specifikaci CipherSpec , musíte získat odpovídající digitální certifikát pro danou specifikaci CipherSpec.

Algoritmus digitálního podpisu MD5 a TLS 1.2

Digitální certifikáty podepsané pomocí algoritmu MD5 jsou odmítnuty při použití protokolu TLS 1.2 . Důvodem je skutečnost, že algoritmus MD5 je nyní mnoha kryptografickými analytiky považován za slabý a jeho použití je obecně nevhodné. Chcete-li použít novější specifikace CipherSpecs založené na protokolu TLS 1.2 , ujistěte se, že digitální certifikáty nepoužívají ve svých digitálních podpisech algoritmus MD5 . Starší specifikace CipherSpecs , které používají protokoly TLS 1.0 , nepodléhají tomuto omezení a mohou i nadále používat certifikáty s digitálními podpisy MD5 .

Chcete-li zobrazit algoritmus digitálního podpisu pro konkrétní certifikát, můžete použít příkaz **runmqakm** :

```
runmqakm -cert -details -db key.kdb -pw password -label cert_label
```

kde *cert_label* je popisek certifikátu algoritmu digitálního podpisu, který se má zobrazit. Podrobnosti viz Popisky digitálních certifikátů .

Poznámka: Ačkoli lze grafické rozhraní **runmqckm** (iKeycmd) a **strmqikm** (iKeyman) použít k zobrazení výběru algoritmů digitálního podpisu, nástroj **runmqakm** poskytuje širší rozsah.

Spuštění příkazu **runmqakm** vytvoří výstup zobrazující použití uvedeného podpisového algoritmu:

```
Label : ibmmqexample
Key Size : 1024
Version : X509 V3
Serial : 4e4e93f1
Issuer : CN=Old Certificate Authority,OU=Test,O=Example,C=US
Subject : CN=Example Queue Manager,OU=Test,O=Example,C=US
Not Before : August 19, 2011 5:48:49 PM GMT+01:00
Not After : August 18, 2012 5:48:49 PM GMT+01:00
Public Key
    30 81 9F 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01
    05 00 03 81 8D 00 30 81 89 02 81 81 00 98 5A 7A
    F0 18 21 EE E4 8A 6E DE C8 01 4B 3A 1E 41 90 3D
    CE 01 3F E6 32 30 6C 23 59 F0 FE 78 6D C2 80 EF
    BC 83 54 7A EB 60 80 62 6B F1 52 FE 51 9D C1 61
    80 A5 1C D4 F0 76 C7 15 6D 1F 0D 4D 31 3E DC C6
    A9 20 84 6E 14 A1 46 7D 4C F5 79 4D 37 54 0A 3B
    A9 74 ED E7 8B 0F 80 31 63 1A 0B 20 A5 99 EE 0A
    30 A6 B6 8F 03 97 F6 99 DB 6A 58 89 7F 27 34 DE
    55 08 29 D8 A9 6B 46 E6 02 17 C3 13 D3 02 03 01
    00 01
Public Key Type : RSA (1.2.840.113549.1.1.1)
Fingerprint : SHA1 :
    09 4E 4F F2 1B CB C1 F4 4F 15 C9 2A F7 32 0A 82
    DA 45 92 9F
Fingerprint : MD5 :
    44 54 81 7C 58 68 08 3A 5D 75 96 40 D5 8C 7A CB
Fingerprint : SHA256 :
    3B 47 C6 E7 7B B0 FF 85 34 E7 48 BE 11 F2 D4 35
    B7 9A 79 53 2B 07 F5 E7 65 E8 F7 84 E0 2E 82 55
Signature Algorithm : MD5WithRSASignature (1.2.840.113549.1.1.4)
Value
    3B B9 56 E6 F2 77 94 69 5B 3F 17 EA 7B 19 D0 A2
    D7 10 38 F1 88 A4 44 1B 92 35 6F 3B ED 99 9B 3A
    A5 A4 FC 72 25 5A A9 E3 B1 96 88 FC 1E 9F 9B F1
    C5 E8 8E CF C4 8F 48 7B 0E A6 BB 13 AE 2B BD D8
    63 2C 03 38 EF DC 01 E1 1F 7A 6F FB 2F 65 74 D0
    FD 99 94 BA B2 3A D5 B4 89 6C C1 2B 43 6D E2 39
    66 6A 65 CB C3 C4 E2 CC F5 49 39 A3 8B 93 5A DD
    B0 21 0B A8 B2 59 5B 24 59 50 44 89 DC 78 19 51
Trust Status : Enabled
```

Řádek `Signature Algorithm` ukazuje, že se používá algoritmus `MD5WithRSASignature` . Tento algoritmus je založen na MD5 , a proto tento digitální certifikát nelze použít se specifikacemi TLS 1.2 CipherSpecs.

Interoperabilita specifikací Elliptic Curve a RSA CipherSpecs

Ne všechny specifikace CipherSpecs lze použít se všemi digitálními certifikáty. CipherSpecs jsou označeny předponou názvu CipherSpec . Každý typ CipherSpec ukládá různá omezení pro typ digitálního certifikátu, který lze použít. Tato omezení se vztahují na všechna připojení TLS produktu IBM MQ , ale jsou zvláště relevantní pro uživatele šifrování Elliptic Curve.

Následující tabulka shrnuje vztahy mezi CipherSpecs a digitálními certifikáty:

Tabulka 4. Vztahy mezi CipherSpecs a digitálními certifikáty

Typ	CipherSpec Předpona názvu	Popis	Požadovaný typ veřejného klíče	Algoritmus šifrování digitálního podpisu	Metoda zavedení tajného klíče
1	ECDHE_ECDSA_	CipherSpecs , které používají veřejné klíče Elliptic Curve, tajné klíče Elliptic Curve a algoritmy digitálního podpisu Elliptic Curve.	Eliptická křivka	ECDSA	ECDHE

Tabulka 4. Vztahy mezi CipherSpecs a digitálními certifikáty (pokračování)

Typ	CipherSpec Předpona názvu	Popis	Požadovaný typ veřejného klíče	Algoritmus šifrování digitálního podpisu	Metoda zavedení tajného klíče
2	ECDHE_RSA_	CipherSpecs , které používají veřejné klíče RSA, tajné klíče Elliptic Curve a algoritmy digitálního podpisu RSA.	RSA	RSA	ECDHE
3	(Všechny specifikace TLS 1.3 CipherSpecs)	CipherSpecs , které používají veřejné klíče Elliptic Curve nebo RSA, tajné klíče Elliptic Curve a algoritmy digitálního podpisu Elliptic Curve nebo RSA.	Eliptická křivka nebo RSA	ECDSA nebo RSA	ECDHE nebo RSA
4	(Všechny ostatní)	CipherSpecs , které používají veřejné klíče RSA a algoritmy digitálního podpisu RSA.	RSA	RSA	RSA

Poznámka: Specifikace CipherSpecs typu 1 a 2 nejsou podporovány správci front IBM MQ a klienty MQI na platformě IBM i .

Požadovaný sloupec typu veřejného klíče zobrazuje typ veřejného klíče, který musí mít osobní certifikát při použití každého typu CipherSpec. Osobní certifikát je certifikát koncové entity, který identifikuje správce front nebo klienta pro svého vzdáleného partnera.

Musíte se ujistit, že certifikát, který je uveden v popisku certifikátu, je vhodný pro kanál CipherSpec. To znamená, že pokud konfigurujete kanál s CipherSpec , která vyžaduje certifikát EC (Elliptic Curve), nemůžete pojmenovat certifikát RSA v popisku certifikátu. Pokud konfigurujete kanál se specifikací CipherSpec , která vyžaduje certifikát RSA, nemůžete v popisku certifikátu pojmenovat certifikát EC.

Za předpokladu, že jste správně nakonfigurovali IBM MQ, můžete mít:

- Jeden správce front se směsicí certifikátů RSA a EC.
- Různé kanály ve stejném správci front používající buď certifikát RSA, nebo certifikát EC.

Šifrovací algoritmus digitálního podpisu odkazuje na šifrovací algoritmus použitý k ověření rovnocenného partnera. Šifrovací algoritmus se používá spolu s hašovacím algoritmem, jako např. MD5, SHA-1 nebo SHA-256 , k výpočtu digitálního podpisu. Existují různé algoritmy digitálního podpisu, které lze použít, například RSA s MD5 nebo ECDSA s SHA-256. V tabulce se ECDSA odkazuje na sadu algoritmů digitálního podpisu, které používají ECDSA; RSA odkazuje na sadu algoritmů digitálního podpisu, které používají RSA. Lze použít jakýkoli podporovaný algoritmus digitálního podpisu v sadě za předpokladu, že je založen na uvedeném šifrovacím algoritmu.

Typ 1 CipherSpecs vyžaduje, aby osobní certifikát měl veřejný klíč Elliptic Curve. Při použití těchto CipherSpecs je k vytvoření tajného klíče pro připojení použita dohoda s přechodným klíčem Elliptic Curve Diffie Hellman Ephemeral key.

Typ 2 CipherSpecs vyžaduje, aby osobní certifikát měl veřejný klíč RSA. Při použití těchto CipherSpecs je k vytvoření tajného klíče pro připojení použita dohoda s přechodným klíčem Elliptic Curve Diffie Hellman Ephemeral key.

Specifikace CipherSpecs typu 3 vyžadují, aby osobní certifikát měl veřejný klíč RSA. Při použití těchto CipherSpecs se k vytvoření tajného klíče pro připojení používá výměna klíčů RSA.

Tento seznam omezení není vyčerpávající: v závislosti na konfiguraci mohou existovat další omezení, která mohou dále ovlivnit schopnost spolupracovat. Je-li například produkt IBM MQ nakonfigurován tak,

aby vyhovoval standardům FIPS 140-2 nebo NSA Suite B, bude to také omezovat rozsah povolených konfigurací. Další informace naleznete v následující části.

Potřebujete-li použít různé typy CipherSpec ve stejném správci front nebo klientské aplikaci, konfigurujte odpovídající popisek certifikátu a kombinaci CipherSpec v definici klienta.

Tři typy CipherSpec nespolupracují přímo: jedná se o omezení aktuálních standardů TLS. Předpokládejme například, že jste zvolili použití volby ECDHE_ECDSA_AES_128_CBC_SHA256 CipherSpec pro přijímací kanál s názvem TO.QM1 ve správci front s názvem QM1, pak by měl mít příjemce osobní certifikát s klíčem Elliptic Curve a digitálním podpisem založeným na ECDSA. Pokud přijímací kanál tyto požadavky nesplňuje, kanál se nespustí.

Ostatní kanály připojující se ke správci front QM1 mohou používat jiné CipherSpecsza předpokladu, že každý kanál používá certifikát správného typu pro CipherSpec daného kanálu. Předpokládejme například, že QM1 používá odesílací kanál s názvem TO.QM2 pro odesílání zpráv jinému správci front s názvem QM2. Kanál TO.QM2 může používat CipherSpec TLS_RSA_WITH_AES_256_CBC_SHA256 typu 3 za předpokladu, že oba konce kanálu používají certifikáty obsahující veřejné klíče RSA. Atribut kanálu popisků certifikátů lze použít ke konfiguraci jiného certifikátu pro každý kanál.

Při plánování sítí IBM MQ pečlivě zvažte, které kanály vyžadují protokol TLS, a ujistěte se, že typ certifikátů používaných pro každý kanál je vhodný pro použití se specifikací CipherSpec na daném kanálu.

Chcete-li zobrazit algoritmus digitálního podpisu a typ veřejného klíče pro digitální certifikát, můžete použít příkaz **runmqakm** :

```
runmqakm -cert -details -db key.kdb -pw password -label cert_label
```

kde *cert_label* je popisek certifikátu, jehož algoritmus digitálního podpisu potřebujete zobrazit. Podrobnosti viz Popisky digitálních certifikátů .

Spuštění příkazu **runmqakm** vytvoří výstup zobrazující typ veřejného klíče:

```
Label : ibmmqexample
Key Size : 384
Version : X509 V3
Serial : 9ad5eeef5d756f41
Issuer : CN=Example Certificate Authority,OU=Test,O=Example,C=US
Subject : CN=Example Queue Manager,OU=Test,O=Example,C=US
Not Before : 21 August 2011 13:10:24 GMT+01:00
Not After : 21 August 2012 13:10:24 GMT+01:00
Public Key
    30 76 30 10 06 07 2A 86 48 CE 3D 02 01 06 05 2B
    81 04 00 22 03 62 00 04 3E 6F A9 06 B6 C3 A0 11
    F8 D6 22 78 FE EF 0A FE 34 52 C0 8E AB 5E 81 73
    D0 97 3B AB D6 80 08 E7 31 E9 18 3F 6B DE 06 A7
    15 D6 9D 5B 6F 56 3B 7F 72 BB 6F 1E C9 45 1C 46
    60 BE F2 DC 1B AD AC EC 64 4C 0E 06 65 6E ED 93
    B8 F5 95 E0 F9 2A 05 D6 21 02 BD FB 06 63 A1 CC
    66 C6 8A 0A 5C 3F F7 D3
Public Key Type : EC_ecPublicKey (1.2.840.10045.2.1)
Fingerprint : SHA1 :
    3C 34 58 04 5B 63 5F 5C C9 7A E7 67 08 2B 84 43
    3D 43 7A 79
Fingerprint : MD5 :
    49 13 13 E1 B2 AC 18 9A 31 41 DC 8C B4 D6 06 68
Fingerprint : SHA256 :
    6F 76 78 68 F3 70 F1 53 CE 39 31 D9 05 C5 C5 9F
    F2 B8 EE 21 49 16 1D 90 64 6D AC EB 0C A7 74 17
Signature Algorithm : EC_ecdsa_with_SHA384 (1.2.840.10045.4.3.3)
Value
    30 65 02 30 0A B0 2F 72 39 9E 24 5A 22 FE AC 95
    0D 0C 6D 6C 2F B3 E7 81 F6 C1 36 1B 9A B0 6F 07
    59 2A A1 4C 02 13 7E DD 06 D6 FE 4B E4 03 BC B1
    AC 49 54 1E 02 31 00 90 0E 46 2B 04 37 EE 2C 5F
    1B 9C 69 E5 99 60 84 84 10 71 1A DA 63 88 33 E2
    22 CC E6 1A 4E F4 61 CC 51 F9 EE A0 8E F4 DC B5
    0B B9 72 58 C3 C7 A4
Trust Status : Enabled
```

Řádek Typ veřejného klíče v tomto případě ukazuje, že certifikát má veřejný klíč Elliptic Curve. Řádek podpisového algoritmu v tomto případě ukazuje, že se používá algoritmus EC_ecdsa_with_SHA384 : je založen na algoritmu ECDSA. Tento certifikát je proto vhodný pouze pro použití se specifikacemi typu 1 CipherSpecs.

Můžete také použít příkaz **runmqckm** se stejnými parametry. Grafické rozhraní produktu **strmqikm** lze také použít k zobrazení algoritmů digitálního podpisu, pokud otevřete úložiště klíčů a poklepejte na popisek certifikátu. Měli byste však použít nástroj **runmqakm** k zobrazení digitálních certifikátů, protože podporuje širší rozsah algoritmů.

TLS 1.3 CipherSpecs

TLS 1.3 CipherSpecs podporují certifikáty ECDSA i RSA.

Eliptické křivky CipherSpecs a NSA Suite B

Když je produkt IBM MQ nakonfigurován tak, aby odpovídal profilu TLS 1.2 kompatibilnímu se standardem Suite B, povolené specifikace CipherSpecs a algoritmy digitálního podpisu jsou omezeny, jak je popsáno v tématu “Šifrování NSA Suite B v IBM MQ” na stránce 41. Kromě toho je rozsah přijatelných klíčů eliptické křivky snížen podle nakonfigurovaných úrovní zabezpečení.

Na 128bitové úrovni zabezpečení Suite B je veřejný klíč subjektu certifikátu vyžadován pro použití eliptické křivky NIST P-256 nebo NIST P-384 a pro podepsání pomocí eliptické křivky NIST P-256 nebo eliptické křivky NIST P-384 . Příkaz **runmqakm** lze použít k vyžádání digitálních certifikátů pro tuto úroveň zabezpečení pomocí parametru -sig_alg EC_ecdsa_with_SHA256nebo EC_ecdsa_with_SHA384.

Na úrovni zabezpečení 192bitové sady Suite B je veřejný klíč subjektu certifikátu vyžadován pro použití eliptické křivky NIST P-384 a pro podepsání eliptickou křivkou NIST P-384 . Příkaz **runmqakm** lze použít k vyžádání digitálních certifikátů pro tuto úroveň zabezpečení pomocí parametru -sig_alg hodnoty EC_ecdsa_with_SHA384.

Podporované eliptické křivky NIST jsou následující:

Tabulka 5. Podporované eliptické křivky NIST

Název křivky NIST FIPS 180-3	**Název křivky RFC 4492**	**Velikost klíče eliptické křivky (bity)**
P-256	secp256r1	256
P-384	secp384r1	384
P-521	secp521r1	521

Poznámka: Eliptickou křivku NIST P-521 nelze použít pro operace vyhovující standardu Suite B.

Související pojmy

“Povolení CipherSpecs” na stránce 438
Povolte CipherSpec pomocí parametru **SSLCIPH** v příkazu **DEFINE CHANNEL** nebo **ALTER CHANNEL** MQSC.

“Určení, že se za běhu v klientu MQI používají pouze specifikace CipherSpecs s certifikací FIPS.” na stránce 270
Vytvořte úložiště klíčů pomocí softwaru vyhovujícího standardu FIPS a poté určete, že kanál musí používat specifikace CipherSpecss certifikací FIPS.

“Šifrování NSA Suite B v IBM MQ” na stránce 41
Toto téma poskytuje informace o tom, jak nakonfigurovat produkt IBM MQ for AIX, Linux, and Windows tak, aby odpovídal profilu TLS 1.2 vyhovujícímu standardu Suite B.

“Národní bezpečnostní agentura (NSA) Suite B kryptografie” na stránce 23
Vláda Spojených států amerických poskytuje technické poradenství v oblasti systémů IT a bezpečnosti, včetně šifrování dat. Americká národní bezpečnostní agentura (NSA) doporučuje ve svém standardu Suite B sadu interoperabilních šifrovacích algoritmů.

Záznamy ověření kanálu

Chcete-li zlepšit kontrolu nad udílením přístupu k připojujícím se systémům na úrovni kanálu, můžete použít záznamy ověření kanálu.

Klienti se mohou pokoušet o připojení k danému správci front pomocí prázdného ID uživatele nebo ID uživatele vysoké úrovně, což by jim umožnilo provádět nežádoucí akce. Přístup těchto klientů lze blokovat pomocí záznamů ověřování kanálu. Případně může klient deklarovat ID uživatele, které je platné na platformě klienta, ale na platformě serveru je neznámé nebo má neplatný formát. Pomocí záznamu ověřování kanálu můžete deklarované ID uživatele mapovat na platné ID uživatele.

Můžete zjistit aplikaci klienta, která se připojuje k danému správci front a chová se v nějakém ohledu nežádoucím způsobem. Chcete-li server ochránit před problémy, které tato aplikace působí, je nutné ji dočasně blokovat pomocí adresy IP aplikace klienta, dokud nedojde k aktualizaci pravidel brány firewall nebo k opravě dané aplikace klienta. Pomocí záznamu ověřování kanálu můžete blokovat adresu IP, z níž se daná aplikace klienta připojuje.

Pokud jste pro tento účel nastavili kanál a nástroj pro administraci, například produkt IBM MQ Explorer, může být vhodné zajistit, aby jej mohly používat jenom specifické počítače klienta. K povolení použití kanálu pouze z určitých adres IP je možné použít záznam ověřování kanálu.

Pokud právě začínáte s některými ukázkovými aplikacemi spuštěnými jako klienti, přečtěte si téma Příprava a spuštění ukázkových programů , kde naleznete příklad bezpečného nastavení správce front pomocí záznamů ověřování kanálu.

Chcete-li získat záznamy ověření kanálu pro řízení příchozích kanálů, použijte příkaz MQSC **ALTER QMGR CHLAUTH(ENABLED)**.

Pravidla **CHLAUTH** se použijí pro kanál MCA kanálu, který je vytvořen jako odezva na nové příchozí připojení. V případě kanálu MCA vytvořeného v reakci na lokálně spuštěný kanál se nepoužijí žádná pravidla **CHLAUTH**.

Tabulka 6. Kde se použijí pravidla CHLAUTH pro různé dvojice kanálů

Typ kanálu	**MCA, kde jsou použita pravidla CHLAUTH**
SDR-RCVR	RCVR
RQSTR-SVR (Spuštěno v SVR)	RQSTR
RQSTR-SVR (Spuštěno v RQSTR)	SVR
RQSTR-SDR (Spuštěno v SDR)	RQSTR
RQSTR-SDR (Spuštěno v RQSTR)	SDR pro počáteční připojení. RQSTR pro připojení zpětného volání.

Je možné vytvořit záznamy ověření kanálu k provádění následujících funkcí:

- Blokování připojení ze specifických adres IP
- Blokování připojení od specifických ID uživatele
- Nastavení hodnoty MCAUSER pro všechny kanály, které se připojují ze specifické adresy IP
- Nastavení hodnoty MCAUSER pro všechny kanály, které deklarují specifické ID uživatele
- Nastavení hodnoty MCAUSER pro všechny kanály, které mají specifický rozlišující název SSL nebo TLS
- Nastavení hodnoty MCAUSER pro všechny kanály, které se připojují ze specifického správce front
- Blokování připojení, která jsou označena jako připojení z konkrétních správců front, pokud se nejedná o připojení ze specifické adresy IP
- Blokování připojení, která prezentují konkrétní certifikát SSL nebo TLS, pokud se nejedná o připojení ze specifické adresy IP

Tyto způsoby použití jsou dále popsány v následujících sekcích.

Záznamy ověřování kanálu vytváříte, upravujete nebo odebírejte pomocí příkazu MQSC **SET CHLAUTH** nebo pomocí příkazu PCF **Set Channel Authentication Record**.

Poznámka: Velký počet záznamů ověřování kanálu může mít negativní dopad na výkon správce front.

Blokování adres IP

Zabránění přístupu ze specifických adres IP je obvykle v kompetenci brány firewall. Může však dojít k situacím, kdy dochází k pokusům o připojení z adres IP, které by neměly mít přístup k vašemu systému IBM MQ. Tyto adresy musí být dočasně blokovány, dokud nedojde k aktualizaci brány firewall. Tyto pokusy o připojení ani nemůžou pocházet z kanálů produktu IBM MQ, ale z jiných soketových aplikací; které jsou nesprávně nakonfigurované pro zaměření vašeho modulu listener produktu IBM MQ. Adresy IP můžete blokovat nastavením záznamu ověřování kanálu typu BLOCKADDR. Můžete zadat jednu nebo více adres, rozsahy adres či vzorce zahrnující zástupné znaky.

Pokud dojde k odmítnutí příchozího připojení kvůli blokování adresy IP tímto způsobem, vydá se zpráva události MQRC_CHANNEL_BLOCKED s kvalifikátorem příčiny MQRQ_CHANNEL_BLOCKED_ADDRESS, za předpokladu, že jsou události kanálu povoleny a správce front je spuštěný. Navíc je připojení ponecháno otevřené po dobu 30 sekund před vydáním chyby, aby se zajistilo, že nedojde k zaplavení modulu listener opakovanými pokusy o připojení, které jsou zablokovány.

Chcete-li zablokovat adresy IP pouze na specifických kanálech nebo chcete-li se vyhnout zpoždění před nahlášením chyby, nastavte záznam ověření kanálu typu ADDRESSMAP s parametrem USERSRC(NOACCESS).

Pokud dojde k odmítnutí příchozího připojení z této příčiny, vydá se zpráva události MQRC_CHANNEL_BLOCKED s kvalifikátorem příčiny MQRQ_CHANNEL_BLOCKED_NOACCESS, za předpokladu, že události kanálu jsou povoleny a správce front je spuštěný.

Příklad najdete v části “Blokování specifických adres IP” na stránce 403.

Blokování ID uživatelů

Chcete-li zabránit konkrétním ID uživatelů v připojení prostřednictvím kanálu klienta, nastavte záznam ověřování kanálu typu BLOCKUSER. Tento typ záznamu ověřování kanálu se vztahuje pouze na kanály klienta, nikoli na kanály zpráv. Je možné zadat jedno nebo více jednotlivých ID uživatelů, která mají být blokována, ale nelze použít zástupné znaky.

Pokud dojde k odmítnutí příchozího připojení z této příčiny, je vydána zpráva události MQRC_CHANNEL_BLOCKED s kvalifikátorem příčiny MQRQ_CHANNEL_BLOCKED_USERID za předpokladu, že jsou povoleny události kanálu.

Příklad najdete v části “Blokování specifických ID uživatelů” na stránce 405.

Dále můžete blokovat libovolný přístup pro konkrétní ID uživatelů v určitých kanálech pomocí nastavení záznamu ověřování kanálu typu USERMAP s parametrem USERSRC(NOACCESS).

Pokud dojde k odmítnutí příchozího připojení z této příčiny, vydá se zpráva události MQRC_CHANNEL_BLOCKED s kvalifikátorem příčiny MQRQ_CHANNEL_BLOCKED_NOACCESS, za předpokladu, že události kanálu jsou povoleny a správce front je spuštěný.

Příklad najdete v části “Blokování přístupu pro ID uživatele klienta” na stránce 408.

Blokování názvů správce front

Chcete-li určit, že kanál připojující se ze zadaného správce front nemá mít přístup, nastavte záznam ověřování kanálu typu QMGRMAP s parametrem USERSRC(NOACCESS). Můžete zadat jeden název správce front nebo vzorec zahrnující zástupné znaky. Při blokování přístupu ze správců front neexistuje ekvivalent funkce BLOCKUSER.

Pokud dojde k odmítnutí příchozího připojení z této příčiny, vydá se zpráva události MQRC_CHANNEL_BLOCKED s kvalifikátorem příčiny MQRQ_CHANNEL_BLOCKED_NOACCESS, za předpokladu, že události kanálu jsou povoleny a správce front je spuštěný.

Příklad najdete v části “Blokování přístupu ze vzdáleného správce front” na stránce 407.

Blokování rozlišujících názvů SSL nebo TLS

Chcete-li určit, že uživatel prezentující osobní certifikát SSL nebo TLS obsahující zadaný rozlišující název nemá mít přístup, nastavte záznam ověřování kanálu typu SSLPEERMAP s parametrem USERSRC(NOACCESS). Můžete zadat jeden rozlišující název nebo vzorec zahrnující zástupné znaky. Při blokování přístupu pro rozlišující názvy neexistuje ekvivalent funkce BLOCKUSER.

Pokud dojde k odmítnutí příchozího připojení z této příčiny, vydá se zpráva události MQRC_CHANNEL_BLOCKED s kvalifikátorem příčiny MQRQ_CHANNEL_BLOCKED_NOACCESS, za předpokladu, že události kanálu jsou povoleny a správce front je spuštěný.

Příklad najdete v části "Blokování přístupu pro rozlišující název SSL nebo TLS" na stránce 408.

Mapování adres IP na používaná ID uživatele

Chcete-li určit, že kanál připojující se ze zadané adresy IP má používat specifický atribut MCAUSER, nastavte záznam ověřování kanálu typu ADDRESSMAP. Můžete zadat jednu adresu, rozsah adres nebo vzorec se zástupnými znaky.

Pokud použijete přesměrování portů, přerušení relace DMZ nebo libovolné jiné nastavení, které mění adresu IP prezentovanou správci front, použití mapování adres IP není nutně vhodné.

Příklad najdete v části "Mapování adresy IP na ID uživatele MCAUSER" na stránce 409.

Mapování názvů správce front na používaná ID uživatele

Chcete-li určit, že kanál připojující se ze zadaného správce front má používat specifický atribut MCAUSER, nastavte záznam ověřování kanálu typu QMGRMAP. Můžete zadat jeden název správce front nebo vzorec zahrnující zástupné znaky.

Příklad najdete v části "Mapování vzdáleného správce front na ID uživatele MCAUSER" na stránce 405.

Mapování ID uživatelů deklarovaných klientem na používaná ID uživatele

Chcete-li určit, že v případě použití konkrétního ID uživatele připojením z klienta IBM MQ MQI se má použít jiný určený uživatel MCAUSER, nastavte záznam ověření kanálu na typ USERMAP. Mapování ID uživatele nepoužívá žádné zástupné znaky.

Příklad najdete v části "Mapování ID uživatele klienta na ID uživatele MCAUSER" na stránce 406.

Mapování rozlišujících názvů SSL nebo TLS na používaná ID uživatele

Chcete-li určit, že uživatel prezentující osobní certifikát SSL/TLS obsahující zadaný rozlišující název má používat specifický atribut MCAUSER, nastavte záznam ověřování kanálu typu SSLPEERMAP. Můžete zadat jeden rozlišující název nebo vzorec zahrnující zástupné znaky.

Příklad najdete v části "Mapování rozlišujícího názvu SSL nebo TLS na ID uživatele MCAUSER" na stránce 407.

Mapování správců front, klientů nebo rozlišovacích názvů SSL nebo TLS podle adresy IP

Za určitých okolností může třetí strana podvrhnout název správce front. Může také dojít ke krádeži a opětovnému použití souboru databáze klíčů či certifikátu SSL nebo TLS. Za účelem ochrany před těmito hrozbami můžete určit, že připojení z určitého správce front nebo klienta nebo pomocí konkrétního rozlišujícího názvu se musí připojovat ze zadané adresy IP. Nastavte záznam ověření kanálu typu USERMAP, QMGRMAP nebo SSLPEERMAP a pomocí parametru ADDRESS zadejte povolenou adresu IP nebo vzorec adres IP.

Příklad najdete v části "Mapování vzdáleného správce front na ID uživatele MCAUSER" na stránce 405.

Interakce mezi záznamy ověření kanálu

Kanál, který se pokouší o připojení, může odpovídat více záznamům ověřování kanálu, které mohou mít protichůdný efekt. Například kanál může deklarovat ID uživatele, které je blokování záznamem ověřování

kanálu BLOCKUSER, ale s certifikátem SSL nebo TLS, který se shoduje se záznamem SSLPEERMAP určujícím jiné ID uživatele. Dále, pokud záznamy ověření kanálu používají zástupné znaky, může jedna adresa IP, název správce front či rozlišující název SSL nebo TLS odpovídat několika vzorcům. Například, adresa IP 192.0.2.6 odpovídá vzorům 192.0.2.0-24, 192.0.2.* a 192.0.*.6. Provedená akce se určí následujícím způsobem.

- Použitý záznam ověřování kanálu je vybrán následovně:
  - Záznam ověřování kanálu, který se přesně shoduje s názvem kanálu, má přednost před záznamem ověřování kanálu, který danému názvu kanálu vyhovuje při použití zástupného znaku.
  - Záznam ověřování kanálu používající rozlišující název SSL nebo TLS má přednost před záznamem používajícím ID uživatele, název správce front nebo adresu IP.
  - Záznam ověřování kanálu používající ID uživatele nebo název správce front má přednost před záznamem používajícím adresu IP.
- Pokud dojde k nalezení vyhovujícího záznamu ověřování kanálu, který určuje atribut MCAUSER, tento atribut MCAUSER je ke kanálu přiřazen.
- Pokud dojde k nalezení vyhovujícího záznamu ověřování kanálu, který určuje, že kanál nemá žádný přístup, je tomuto kanálu přiřazena hodnota *NOACCESS atributu MCAUSER. Tuto hodnotu lze později změnit pomocí uživatelské procedury zabezpečení zprávy.
- Pokud nedojde k nalezení vyhovujícího záznamu ověřování kanálu nebo pokud je nalezen vyhovující záznam ověřování kanálu, který určuje ID uživatele kanálu, který má být použit, dojde k prozkoumání pole MCAUSER.
  - Pokud je pole MCAUSER prázdné, dojde k přiřazení ID uživatele klienta k danému kanálu.
  - Pokud pole MCAUSER není prázdné, bude přiřazeno k danému kanálu.
- Dále dojde ke spuštění uživatelských procedur pro zabezpečení zprávy. Tento uživatelský program může nastavit ID uživatele kanálu nebo určit, že přístup má být blokován.
- Pokud je připojení blokování nebo pokud je atribut MCAUSER nastaven na hodnotu *NOACCESS, kanál bude ukončen.
- Pokud připojení není blokováno, pro libovolný kanál s výjimkou kanálu klienta bude ID uživatele kanálu zjištěné v předchozích krocích porovnáno se seznamem blokovaných uživatelů.
  - Pokud se ID uživatele nachází na seznamu blokovaných uživatelů, kanál bude ukončen.
  - Pokud se ID uživatele nenachází na seznamu blokovaných uživatelů, kanál bude spuštěn.

Tam, kde se shoduje řada záznamů ověřování kanálu s názvem kanálu, adresou IP, názvem hostitele, názvem správce front nebo rozlišovacím názvem SSL nebo DNS, je použita nejlepší shoda. Za shodu se považuje:

- Nejlepší je název bez zástupných znaků, např.:
  - Kanál názvu A.B.C.
  - Adresa IP 192.0.2.6.
  - Název hostitele produktu `hursley.ibm.com`
  - Název správce front 192.0.2.6.
- Nejobecnější shoda je jedna hvězdička (*), která odpovídají, např.:
  - všechny názvy kanálů.
  - všechny adresy IP.
  - Všechny názvy hostitelů.
  - všechny názvy správců front.
- Vzorec s hvězdičkou na začátku řetězce je obecnější, než definovaná hodnota na začátku řetězce:
  - Kanály *.B.C jsou obecnější než A.*
  - Adresy IP *.0.2.6 jsou obecnější než 192.*

  - Pro názvy hostitelů je `*.ibm.com` obecnější než `hursley.*`
  - Názvy správců front *QUEUEMANAGER jsou obecnější než QUEUEMANAGER*
- Vzorec s hvězdičkou na specifickém místě v řetězci je obecnější, než definovaná hodnota na stejném místě v řetězci, a podobně i pro všechny následné pozice v řetězci:
  - Kanály A.*.C jsou obecnější než A.B.*
  - Adresy IP 192.*.2.6 jsou obecnější než 192.0.*.
  - Pro názvy hostitelů je `hursley.*.com` obecnější než `hursley.ibm.*`
  - Názvy správců front Q*MANAGER jsou obecnější než QUEUE*
- Pokud mají dva nebo více vzorců hvězdičku na stejné pozici v řetězci, je obecnější vzorec, kde po hvězdičce následuje méně uzlů:
  - Pro kanály je hodnota A.* obecnější než A.*.C.
  - Pro adresy IP je hodnota 192.* obecnější než 192.*.2.*.
  - Pro názvy hostitelů je `hurlsey.*` obecnější než `hursley.*.com`
  - Názvy správců front Q* jsou obecnější než Q*MGR
- Navíc pro adresy IP:
  - Rozsah určený pomlčkou (-) je konkrétnější než hvězdička. Vzorec 192.0.2.0-24 je tedy konkrétnější než vzorec 192.0.2.*.
  - Rozsah, který je podmnožinou jiného rozsahu, je konkrétnější než větší rozsah. Vzorec 192.0.2.5-15 je tedy konkrétnější než vzorec 192.0.2.0-24.
  - Překrývající se rozsahy nejsou povoleny. Například nelze použít záznamy ověření kanálu pro vzorce 192.0.2.0-15 a 192.0.2.10-20.
  - Vzorec nesmí mít menší než vyžadovaný počet částí, pokud tento vzorec nekončí jednou hvězdičkou. Například, hodnota 192.0.2 je neplatná, ale 192.0.2.* je platná.
  - Koncová hvězdička musí být oddělena od zbývající části adresy příslušným oddělovačem (tečka (.) pro adresu IPv4, dvojtečka (:) pro adresu IPv6). Například vzorec 192.0*, není platný, protože hvězdička není samostatnou částí.
  - Vzorec může obsahovat další hvězdičky, pokud je nejedná o hvězdičky připojené za koncovou hvězdičkou. Například, hodnota 192.*.2.* je platná, ale hodnota 192.0.*.* je neplatný.
  - Vzorec adresy IPv6 nesmí obsahovat dvojtečku a koncovou hvězdičku, protože výsledná adresa by byla nejednoznačná. Například vzorec 2001::* by bylo možné rozšířit na formát 2001:0000:*, 2001:0000:0000:* atd.
- V případě rozlišujícího názvu SSL nebo TLS je pořadí přednosti podřetězců následující:

Tabulka 7. Pořadí přednosti v podřetězcích

Pořadí	Podřetězec rozlišujícího názvu	Název
1	SERIALNUMBER=	Sériové číslo certifikátu
2	MAIL=	E-mailová adresa
3	Deprecated E=	E-mailová adresa (zamítnuto ve prospěch volby MAIL)
4	UID=, USERID=	Identifikátor uživatele
5	CN=	Obecný název
6	T=	Titulek
7	OU=	Organizační jednotka
8	DC=	Komponenta domény

Tabulka 7. Pořadí přednosti v podřetězcích (pokračování)		
Pořadí	**Podřetězec rozlišujícího názvu**	**Název**
9	O=	Organizace
10	STREET=	Ulice/první řádek adresy
11	L=	Lokalita
12	ST=, SP=, S=	název státu nebo správního celku
13	PC=	PSČ
14	C=	Země
15	UNSTRUCTUREDNAME=	Název hostitele
16	UNSTRUCTUREDADDRESS=	Adresa IP
17	DNQ=	Kvalifikátor rozlišujícího názvu

Pokud je tedy certifikát SSL nebo TLS prezentován s rozlišujícím názvem obsahujícím podřetězce O=IBM a C=UK, produkt IBM MQ dá přednost záznamu ověřování kanálu pro volbu O=IBM před volbou C=UK.

Rozlišující název může obsahovat více organizačních jednotek, které musí být zadány v hierarchickém pořadí s největšími organizačními jednotkami zadanými na prvním místě. Pokud jsou dva rozlišující názvy shodné ve všech ohledech kromě hodnot organizační jednotky, konkrétnější rozlišující název bude určen následujícím způsobem:

1. Pokud mají různé počty atributů organizačních jednotek, bude jako konkrétnější považován rozlišující název s vyšším počtem hodnot organizačních jednotek. Důvodem je, že rozlišující název s větším počtem organizačních jednotek určuje daný rozlišující název podrobněji a poskytuje více vyhovujících kritérií. I když je organizační jednotkou na nejvyšší úrovni zástupný znak (OU=*), rozlišující název s více organizačními jednotkami bude stále považován za celkově konkrétnější.
2. Pokud mají stejný počet atributů organizačních jednotek, odpovídající dvojice hodnot organizačních jednotek budou porovnány postupně zleva doprava, kde organizační jednotka nejvíce vlevo má nejvyšší úroveň (je nejméně specifická), podle následujících pravidel.
   a. Organizační jednotka bez hodnot zástupných znaků je nejkonkrétnější, protože jí vyhovuje pouze jeden řetězec.
   b. Organizační jednotka s jedním zástupným znakem na začátku nebo na konci (například OU=ABC* nebo OU=*ABC) je v pořadí konkrétnosti na druhém místě.
   c. Organizační jednotka se dvěma zástupnými znaky (například OU=*ABC*) je v tomto pořadí další.
   d. Organizační jednotka tvořená pouze zástupným znakem (OU=*) je nejméně specifická.
3. Pokud jsou výsledkem porovnání řetězců dvě hodnoty atributů se stejnou mírou konkrétnosti, bude za konkrétnější považován atribut s delším řetězcem.
4. Pokud jsou výsledkem porovnání řetězců dvě hodnoty atributů se stejnou mírou konkrétnosti a délkou, výsledek bude určen porovnáním částí rozlišujících názvů bez zástupných znaků a bez rozlišení velikosti písmen.

Pokud jsou dva rozlišující názvy shodné ve všech ohledech kromě svých hodnot DC, platí stejná pravidla porovnání jako u organizačních jednotek, kromě toho, že v hodnotách DC přestavuje nejnižší úroveň hodnota DC, která je nejvíce vlevo (nejvíce specifická), a dle toho se odpovídajícím způsobem liší pořadí porovnání.

Zobrazení záznamů ověřování kanálu

Chcete-li zobrazit záznamy ověřování kanálu, použijte příkaz MQSC **DISPLAY CHLAUTH** nebo příkaz PCF **Inquire Channel Authentication Records**. Můžete vybrat vrácení všech záznamů, které odpovídají zadanému názvu kanálu, nebo můžete vybrat přesnou shodu. Přesná shoda určuje, který

záznam ověřování kanálu bude použit v případě, že se kanál pokusí o vytvoření připojení ze specifické adresy IP, z konkrétního správce front nebo pomocí zadaného ID uživatele, a volitelně prezentuje osobní certifikát SSL/TLS obsahující zadaný rozlišující název.

Související pojmy

“Zabezpečení pro vzdálený systém zpráv” na stránce 100
Tato část se zabývá aspekty zabezpečení vzdáleného systému zpráv.

Interakce CHLAUTH a CONNAUTH

Jak záznamy ověření kanálu (CHLAUTH) a ověření připojení (CONNAUTH) interaktivně spolupracují v produktu IBM MQv případě jediné konverzace na kanálu.

Různé typy vazeb

Produkt IBM MQ podporuje pro připojení aplikace dvě metody:

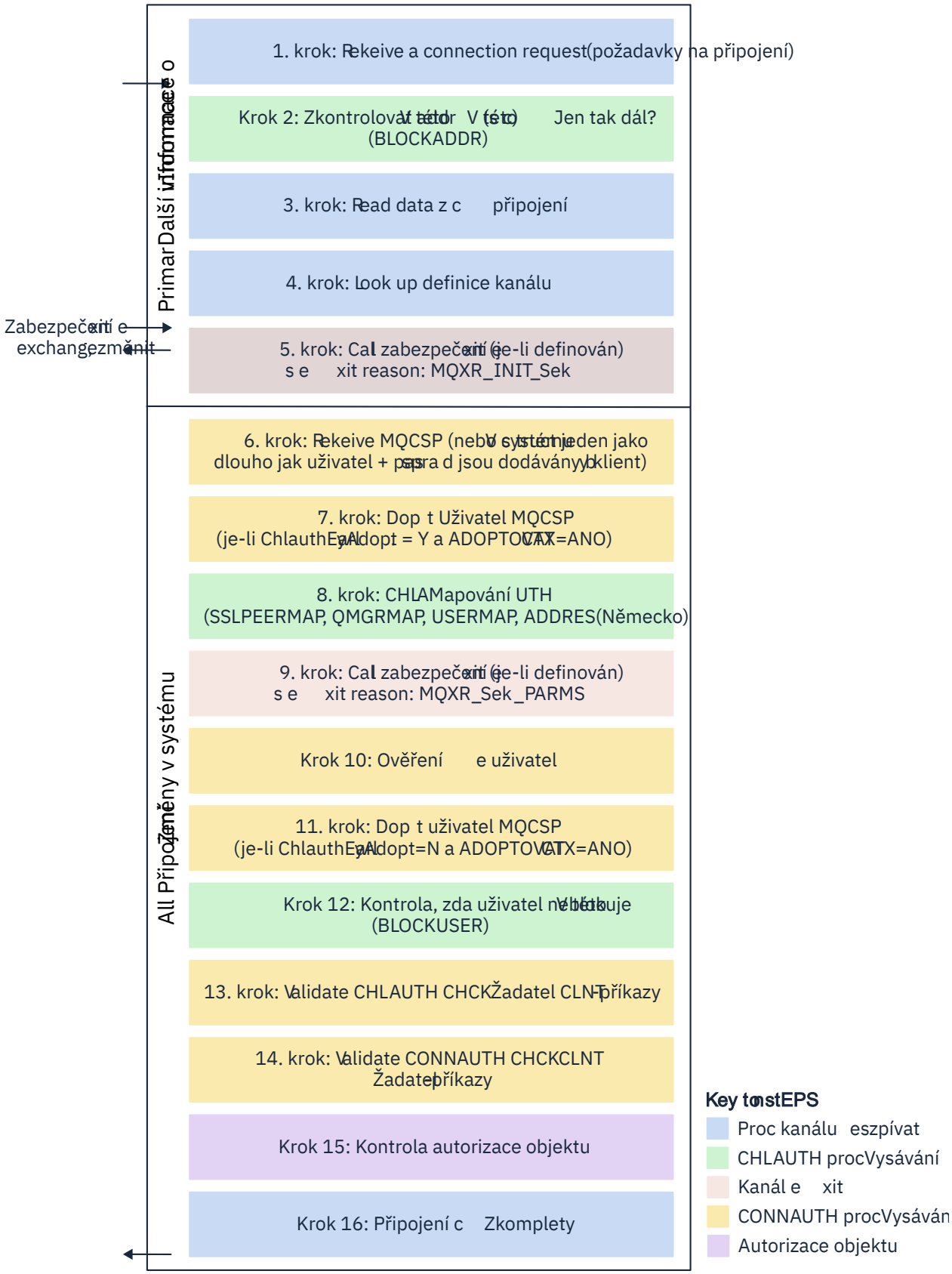
Lokální vazby
: Použije se, pokud se aplikace a správce front nacházejí ve stejném provozním obrazu. CHLAUTH není pro tento typ připojení aplikace relevantní.

Vazby klienta
: Použije se, když aplikace a správce front používají síť ke komunikaci. Aplikace a správce front mohou být spuštěny na stejném počítači nebo mohou být na různých počítačích. V produktu IBM MQje připojení klienta obsluhováno ve formě kanálu připojení serveru (SVRCONN) a v této situaci jsou použitelné jak CONNAUTH, tak CHLAUTH.

Kroky vazby přijímacího konce kanálu

Když se aplikace připojí ke správci front, provede se podstatná kontrola, aby se zajistilo, že oba konce kanálu pochopí, co druhý konec podporuje. Přijímací konec kanálu provádí nějakou další kontrolu, zahrnující CHLAUTH a CONNAUTH, aby se zajistilo, že se klient může připojit, a tento proces může také zahrnovat uživatelskou proceduru zabezpečení, protože to může ovlivnit výsledek. Tato fáze připojení kanálu se také nazývá *fáze vazby*.

V následujícím diagramu jsou uvedeny kroky, kterými kanál SVRCONN prochází při spuštění konce serveru (ve správci front):



Krok 1: Přijetí požadavku na připojení
Inicializátor kanálu nebo modul listener obdrží požadavek na připojení odněkud ze sítě.

Krok 2: Je adresa povolena pro připojení?
Před přečtením jakýchkoli dat produkt IBM MQ zkontroluje adresu IP partnera vůči pravidlům CHLAUTH, aby zjistil, zda je adresa v pravidle *BLOCKADDR* . Není-li adresa nalezena, a není-li tedy blokována, tok pokračuje dalším krokem.

Krok 3: Čtení dat z kanálu
Produkt IBM MQ nyní načte data do vyrovnávací paměti a začne zpracovávat odeslané informace.

Krok 4: Vyhledání definice kanálu
V prvním datovém toku produkt IBM MQ mimo jiné odesílá název kanálu, který se pokouší spustit odesílající konec. Přijímající správce front pak může vyhledat definici kanálu, která obsahuje všechna nastavení určená pro daný kanál.

Krok 5: Zavolejte proceduru zabezpečení (je-li definována)
Je-li pro kanál definována uživatelská procedura pro zabezpečení zprávy (SCYEXIT), je volána s příčinou ukončení (MQCXP.**ExitReason**). nastavit na MQXR_INIT_SEC.

Krok 6: Přijetí MQCSP
Je-li to nutné, vytvořte jedno, pokud klient zadá ověřovací pověření.

Pokud je klientem aplikace Java nebo JMS spuštěná v režimu kompatibility, klient nepředá správci front strukturu MQCSP. Místo toho, pokud aplikace zadala ID uživatele a heslo, je zde vytvořena struktura MQCSP.

Krok 7: Přijetí uživatele MQCSP (má-li parametr `ChlauthEarlyAdopt` hodnotu *Y* a hodnotu ADOPTCTX=YES)
Pověření dodaná klientem jsou ověřena.

Pokud CONNAUTH používá LDAP k mapování deklarovaného rozlišujícího názvu na krátké ID uživatele, mapování proběhne v tomto kroku.

Je-li ověření úspěšné, je ID uživatele převzata kanálem a je použita krokem mapování CHLAUTH.

Poznámka: Parametr IBM MQ 9.0.4 **`ChlauthEarlyAdopt=`** *Y* se automaticky přidá do sekce kanálů souboru qm.ini pro nové správce front.

Krok 8: Mapování CHLAUTH
Mezipaměť CHLAUTH je znovu zkontrolována, aby vyhledala pravidla mapování *SSLPEERMAP*, *USERMAP*, *QMGRMAP*a *ADDRESSMAP*.

Použije se pravidlo, které se nejvíce shoduje s příchozím kanálem. Má-li pravidlo **USERSRC***(CHANNEL)* nebo *(MAP)*, pokračuje kanál ve vazbě.

Pokud se pravidla CHLAUTH vyhodnotí jako pravidlo s **USERSRC***(NOACCESS)*, aplikace se zablokuje v připojení ke kanálu, pokud nejsou pověření následně přepsána platnými pověřeními v kroku 9.

Krok 9: Volat uživatelskou proceduru pro zabezpečení zprávy (je-li definována)
Je-li pro kanál definována uživatelská procedura pro zabezpečení zprávy (SCYEXIT), je volána s příčinou ukončení (MQCXP.**ExitReason**). nastavit na MQXR_SEC_PARMS.

V poli **SecurityParms** struktury MQCXP bude uveden ukazatel na MQCSP .

Struktura MQCSP obsahuje ukazatele na ID uživatele (MQCSP.**CSPUserIdPtr**) a heslo (MQCSP.**CSPPasswordPtr**). V 9.3.4 Ze systému IBM MQ 9.3.4struktura MQCSP také obsahuje ukazatel na token ověření (MQCSP.**TokenPtr**).

V uživatelské proceduře je možné změnit ID uživatele a hesloa token ověření . Následující příklad ukazuje, jak by uživatelská procedura zabezpečení vytiskla hodnoty ID uživatele a hesla do protokolu auditu:

```
if (pMQCXP -> ExitReason == MQXR_SEC_PARMS)
{
  /* It is not a good idea for security reasons to print out the user ID */
  /* and password but the following is shown for demonstration reasons */
  printf("User ID: %.*s Password: %.*s\n",
         pMQCXP -> SecurityParms -> CSPUserIdLength,
         pMQCXP -> SecurityParms -> CSPUserIdPtr,
```

```
        pMQCXP -> SecurityParms -> CSPPasswordLength,
        pMQCXP -> SecurityParms -> CSPPasswordPtr);
```

Uživatelská procedura může sdělit systému IBM MQ , aby kanál zavřel, a to vrácením příkazu *MQXCC_CLOSE_CHANNEL* v prostředí MQCXP.**Exitresponse** pole. Jinak bude zpracování kanálu pokračovat do fáze ověřování připojení.

Poznámka: Pokud je deklarovaný uživatel změněn uživatelskou procedurou zabezpečení, pravidla mapování CHLAUTH se znovu nepoužijí na nového uživatele.

Krok 10: Ověření uživatele

K fázi ověřování dochází v případě, že je ve správci front povolena volba CONNAUTH.

Chcete-li to zkontrolovat, zadejte příkaz MQSC 'DISPLAY QMGR CONNAUTH'.

z/OS Následující příklad ukazuje výstup příkazu **DISPLAY QMGR CONNAUTH** ze správce front spuštěného v systému IBM MQ for z/OS.

```
CSQM201I !MQ25 CSQMDRTC DISPLAY QMGR DETAILS
QMNAME(MQ25)
CONNAUTH(SYSTEM.DEFAULT.AUTHINFO.IDPWOS)
 END QMGR DETAILS
CSQ9022I !MQ25 CSQMDRTC ' DISPLAY QMGR' NORMAL COMPLETION
```

Multi Následující příklad ukazuje výstup příkazu '**DISPLAY QMGR CONNAUTH**' ze správce front spuštěného v systému IBM MQ for Multiplatforms.

```
    1 : DISPLAY QMGR CONNAUTH
AMQ8408: Display Queue Manager details.
   QMNAME(DEMO)
   CONNAUTH(SYSTEM.DEFAULT.AUTHINFO.IDPWOS)
```

Hodnota CONNAUTH je název objektu **AUTHINFO** IBM MQ .

Vzhledem k tomu, že ověření operačního systému (**AUTHTYPE**(*IDPWOS*)) je platné na systémech IBM MQ for Multiplatforms i IBM MQ for z/OS, příklady používají ověření operačního systému.

z/OS Následující příklad ukazuje výchozí objekt AUTHINFO se systémem **AUTHTYPE**(*IDPWOS*) ze správce front spuštěného v systému IBM MQ for z/OS.

```
CSQM293I !MQ25 CSQMDRTC 1 AUTHINFO FOUND MATCHING REQUEST CRITERIA
CSQM201I !MQ25 CSQMDRTC DISPLAY AUTHINFO DETAILS
AUTHINFO(SYSTEM.DEFAULT.AUTHINFO.IDPWOS)
AUTHTYPE(IDPWOS)
QSGDISP(QMGR)
ADOPTCTX(NO)
CHCKCLNT(NONE)
CHCKLOCL(OPTIONAL)
FAILDLAY(1)
DESCR()
ALTDATE(2018-06-04)
ALTTIME(10.43.04)
  END AUTHINFO DETAILS
CSQ9022I !MQ25 CSQMDRTC ' DISPLAY AUTHINFO' NORMAL COMPLETION
```

Multi Následující příklad ukazuje výchozí objekt AUTHINFO se systémem **AUTHTYPE**(*IDPWOS*) ze správce front spuštěného v systému IBM MQ for Multiplatforms.

```
 1 : display authinfo(SYSTEM.DEFAULT.AUTHINFO.IDPWOS)
AMQ8566: Display authentication information details.
   AUTHINFO(SYSTEM.DEFAULT.AUTHINFO.IDPWOS)
   AUTHTYPE(IDPWOS)                        ADOPTCTX(NO)
   DESCR( )                                CHCKCLNT(REQDADM)
   CHCKLOCL(OPTIONAL)                      FAILDLAY(1)
   ALTDATE(2015-06-08)                     ALTTIME(16.35.16)
```

Objekt AUTHINFO TYPE (IDPWOS) má atribut s názvem CHCKCLNT. Je-li hodnota změněna na *REQUIRED* , musí všechny klientské aplikace dodat platná pověření.

Pokud byl uživatel ověřen v kroku 7, další kontrola ověření se neprovede, pokud:

- ID uživatele, heslo nebo token ověření v poli SecurityParms struktury MQCXP bylo změněno uživatelskou procedurou zabezpečení v kroku 9.
- Klientská aplikace se připojila k volbám požadujícím znovu připojitelnou funkčnost.

Krok 11: Přijetí kontextu uživatele MQCSP (Pokud `ChlauthEarlyAdopt=`*N* a když je CTX=YES)
Můžete nastavit atribut ADOPTCTX , který řídí, zda je kanál spuštěn pod MCAUSER, nebo ID uživatele, které aplikace dodala.

Pokud bylo ID uživatele deklarované v MQCSP nebo v poli **`SecurityParms`** struktury MQXCP úspěšně ověřeno a hodnota **ADOPTCTX** je *YES*, bude kontext uživatele vyplývající z kroků 7 a 8 převzat jako kontext, který se má použít pro tuto aplikaci, pokud není ID uživatele, heslo, nebo token ověření v poli **`SecurityParms`** struktury MQCXP byl změněn uživatelskou procedurou pro zabezpečení v kroku 9.

Toto deklarovaný ID uživatele je ID uživatele, u kterého se kontroluje autorizace pro použití prostředků IBM MQ .

Například v kanálu SVRCONN není nastaven uživatel MCAUSER a váš klient je spuštěn v adresáři '`johndoe`' v počítači se systémem Linux . Vaše aplikace určuje uživatele '`fred`' v protokolu MQCSP, takže kanál začíná pracovat s uživatelem '`johndoe`' jako aktivním uživatelem MCAUSER. Po kontrole CONNAUTH je uživatel '`fred`' adoptován a kanál je spuštěn s '`fred`' jako aktivní MCAUSER.

Krok 12: Zkontrolujte, zda není uživatel blokován (BLOCKUSER)
Pokud je kontrola CONNAUTH úspěšná, je mezipaměť CHLAUTH znovu zkontrolována, aby se zkontrolovalo, zda je aktivní uživatel MCAUSER blokován pravidlem *BLOCKUSER* . Je-li uživatel blokován, kanál se ukončí.

Krok 13: Ověřit požadavky CHLAUTH CHCKCLNT
Pokud pravidlo CHLAUTH, které bylo vybráno v kroku 8 , dále uvádí hodnotu CHCKCLNT REQUIRED nebo REQDADM, pak se provede ověření, aby se zajistilo, že bylo poskytnuto platné ID uživatele CONNAUTH ke splnění požadavku.

- Je-li nastaven parametr CHCKCLNT (REQUIRED), musí být uživatel ověřen v kroku 7 nebo 10. Jinak je připojení odmítnuto.
- Je-li nastaveno CHCKCLNT (REQDADM), musí být uživatel ověřen v kroku 7 nebo 10 , pokud je toto připojení určeno jako privilegované. Jinak je připojení odmítnuto.
- Je-li nastavena hodnota CHCKCLNT (ASQMGR), bude tento krok vynechán.

Notes:

1. Pokud je nastaveno CHCKCLNT (REQUIRED) nebo CHCKCLNT (REQDADM), ale CONNAUTH není ve správci front povolen, připojení selže s návratovým kódem MQRC_SECURITY_ERROR (2063) kvůli konfliktu v konfiguraci.
2. Uživatel není v tomto kroku znovu ověřen.

Krok 14: Ověřte požadavky na CONNAUTH CHCKCLNT.
K fázi ověřování dochází v případě, že je ve správci front povolena volba CONNAUTH.

Hodnota CONNAUTH CHCKCLNT je kontrolována, aby se zjistilo, jaké požadavky jsou nastaveny pro příchozí připojení:

- Je-li nastaven parametr CHCKCLNT (NONE), bude tento krok vynechán.
- Je-li nastaven parametr CHCKCLNT (OPTIONAL), bude tento krok vynechán.
- Je-li nastaven parametr CHCKCLNT (REQUIRED), musí být uživatel ověřen v kroku 7 nebo 10. Jinak je připojení odmítnuto.
- Je-li nastaveno CHCKCLNT (REQDADM), musí být uživatel ověřen v kroku 7 nebo 10 , pokud je toto připojení určeno jako privilegované. Jinak je připojení odmítnuto.

Poznámka: Uživatel není v tomto kroku znovu ověřen.

Multi **Krok 15: Kontrola autorizace objektu**
Provede se kontrola, zda má aktivní uživatel MCAUSER odpovídající oprávnění pro připojení ke správci front.

ALW Další informace viz Správce oprávnění k objektu.

IBM i Další informace viz “Správce oprávnění k objektu na systému IBM i” na stránce 158.

Krok 16: Připojení je dokončeno
Pokud se předchozí kroky úspěšně dokončí, připojení se dokončí.

Související pojmy
CONNAUTH
Správce front lze nakonfigurovat tak, aby ověřoval pověření dodaná aplikací při připojení.

Související odkazy
NASTAVIT CHLAUTH
ALTER AUTHINFO

Řešení problémů s přístupem CHLAUTH
Kroky a příklady k vyřešení určitých problémů s přístupem při použití záznamů ověření kanálu (CHLAUTH).

Než začnete

Poznámka: Kroky v této úloze vyžadují spuštění příkazů MQSC. Způsob, jakým to provedete, se liší podle platformy. Viz Administrace IBM MQ pomocí příkazů MQSC.

Informace o této úloze

Pro zpracování CHLAUTH existují tři výchozí pravidla:

- ŽÁDNÝ PŘÍSTUP KE VŠEM KANÁLŮM ZE STRANY UŽIVATELŮ `MQ-admin*`
- ŽÁDNÝ PŘÍSTUP KE VŠEM SYSTÉMŮM. * kanály všech uživatelů
- POVOLIT přístup k SYSTEM.ADMIN.SVRCONN (bez uživatelů `MQ-admin`)

První dvě pravidla blokují přístup ke všem kanálům. Třetí pravidlo je specifičtější, a proto má přednost před ostatními dvěma, pokud je kanál SYSTEM.ADMIN.SVRCONN umožňuje přístup k tomuto kanálu.

Pravidla CHLAUTH se používají k určení, zda lze kanál spustit, a umožňují mapování prostřednictvím MCAUSER na jiné ID uživatele. Pokud kanál nelze spustit, obvykle se vyskytnou následující chyby:

- `RC 2035 MQRC_NOT_AUTHORIZED`
- `RC 2059 MQRC_Q_MGR_NOT_AVAILABLE`
- `AMQ4036 Přístup není povolen`
- `AMQ9776: Kanál byl blokován ID uživatele.`
- `AMQ9777: Kanál byl zablokován.`
- `MQJE001: Došlo k výjimce MQException: kód dokončení 2, příčina 2035`
- `MQJE036: Správce front odmítl pokus o připojení.`

Měli byste blokovat přístup striktně, pak přidejte další pravidla CHLAUTH pro kontrolu, kdo může přistupovat a spustit kanály.

Jako dočasný ukazatel a při odstraňování problémů s uvedenými chybami proveďte některý z následujících kroků.

Procedura

- **Zakázat pravidla CHLAUTH**

Jako dočasné opatření a také k odstraňování výše uvedených chyb můžete zakázat pravidla CHLAUTH. Pravidla lze kdykoli znovu povolit, a pokud zakážete pravidla CHLAUTH, vyřeší problém s připojením, víte, že to byla příčina.

Chcete-li zakázat pravidla CHLAUTH, spusťte následující příkaz MQSC:

```
ALTER QMGR CHLAUTH (DISABLED)
```

Všimněte si, že můžete také nastavit CHLAUTH na *WARN*, což umožňuje přístup a protokoluje výsledek pravidla.

- **Upravit nebo odebrat pravidla CHLAUTH**

  Můžete také odstranit nebo upravit pravidlo nebo pravidla CHLAUTH, což způsobí váš problém.

  Chcete-li upravit pravidlo CHLAUTH, použijte příkaz SET CHLAUTH s ACTION (REPLACE). Chcete-li například upravit výchozí pravidlo, které nezpůsobí žádný přístup ke všem kanálům ze strany uživatelů `MQ-admin` k WARN, namísto toho, aby bylo blokováno, spusťte následující příkaz MQSC:

```
SET CHLAUTH (*) TYPE (BLOCKUSER) USERLIST (*MQADMIN) WARN(YES)
ACTION (REPLACE)
```

  Chcete-li odstranit pravidlo CHLAUTH, použijte příkaz SET CHLAUTH s akcí ACTION (REMOVE). Chcete-li například odstranit výchozí pravidlo, které nezpůsobí žádný přístup uživatelů produktu `MQ-admin` ke všem kanálům, spusťte následující příkaz MQSC:

```
SET CHLAUTH (*) TYPE (BLOCKUSER) USERLIST (*MQADMIN) ACTION (REMOVE)
```

- **Test přístupu pomocí MATCH (RUNCHECK)**

  Výsledek pravidel CHLAUTH můžete otestovat pomocí volby MATCH (*RUNCHECK*) pravidla CHLAUTH. Volba **MATCH** (*RUNCHECK*) vrací záznam, který odpovídá specifickému příchozímu kanálu za běhu, pokud se tento kanál připojí k tomuto správci front. Musíte poskytnout:

  – Název kanálu
  – atribut Adresa
  – Atribut SSLPEER, pouze pokud kanál příchozích požadavků používá zabezpečení SSL nebo TLS.
  – QMNAME, pokud je příchozí kanál kanálem správce front, nebo
  – atribut CLNTUSER, pokud je příchozí kanál kanálem klienta

  Následující příklad spustí příkaz MQSC, který zkontroluje, jaké pravidlo CHLAUTH s výchozími pravidly má za následek `MQ-admin` uživatele `johndoe` přistupujícího ke kanálu s názvem `CHAN1`:

```
DISPLAY CHLAUTH (CHAN1) MATCH (RUNCHECK) CLNTUSER ('johndoe') ADDRESS
('192.168.1.138')

AMQ8878: Display channel authentication record details.
CHLAUTH(*) TYPE(BLOCKUSER)
USERLIST(*MQADMIN)
```

  Pro uživatele `johndoe`se kanál nespustí, uživatel bude blokován kvůli pravidlu BLOCKUSER pro uživatele *MQADMIN.

  Následující příklad spustí příkaz MQSC, který zkontroluje, jaké pravidlo CHLAUTH s výchozími pravidly má za následek uživatele `alice` , který není uživatelem produktu `MQ-admin` , přistupujícího ke kanálu s názvem `CHAN1`:

```
DISPLAY CHLAUTH (CHAN1) MATCH (RUNCHECK) CLNTUSER ('alice') ADDRESS
('192.168.1.138')

AMQ9783: Channel will run using MCAUSER('alice').
```

Pro uživatele `alice`je kanál spuštěn a kanál předává `alice` jako MCAUSER. MCAUSER je ID uživatele použité ke kontrole oprávnění k objektu IBM MQ .

Související odkazy
NASTAVIT CHLAUTH
ZOBRAZITYCHLAUTH

Vytvoření nových pravidel CHLAUTH pro uživatele
Některé běžné scénáře pro uživatele a příklad pravidel CHLAUTH k jejich provedení.

Než začnete

Poznámka: Kroky v této úloze vyžadují spuštění příkazů MQSC. Způsob, jakým to provedete, se liší podle platformy. Viz Administrace IBM MQ pomocí příkazů MQSC.

Informace o této úloze

Pro zpracování CHLAUTH existují tři výchozí pravidla:

- ŽÁDNÝ PŘÍSTUP KE VŠEM KANÁLŮM ZE STRANY UŽIVATELŮ `MQ-admin*`
- ŽÁDNÝ PŘÍSTUP KE VŠEM SYSTÉMŮM. * kanály všech uživatelů
- POVOLIT přístup k SYSTEM.ADMIN.SVRCONN (bez uživatelů `MQ-admin`)

První dvě pravidla blokují přístup ke všem kanálům. Třetí pravidlo je specifičtější, a proto má přednost před ostatními dvěma, pokud je kanál SYSTEM.ADMIN.SVRCONN umožňuje přístup k tomuto kanálu.

Chcete-li vytvořit nová pravidla CHLAUTH pro uživatele, nakonfigurujte jeden nebo více následujících scénářů.

Procedura

- **Řízení přístupu pro specifické `MQ-admin` uživatele**
  a) Nastavte kanál připojení serveru, který má být používán výhradně pro administrativní perspektivu, tj. pro připojení z produktu IBM MQ Explorer.

     Máte specifický kanál pro toto použití a definovanou adresu IP nebo adresy, ze kterých chcete přijímat připojení, a přístup blokovaný pro ID `'mqm'` , pokud připojení není z jedné z uvedených adres IP.

  b) Vytvořte kanál SVRCONN pro uživatele IBM MQ Explorer a `MQ-admin` s názvem `ADMIN.CHAN`.

     Spusťte tento příkaz MQSC:

```
DEFINE CHANNEL (ADMIN.CHAN) CHLTYPE (SVRCONN) TRPTYPE (TCP)
```

  c) Pro testování se ujistěte, že máte definovaného uživatele, který je ve skupině `MQ-admin` , a ten, který není.

     Pro tento scénář je `mqadm` ve skupině `MQ-admin` a `alice` není.

  d) Potvrďte, že výchozí pravidla CHLAUTH jsou na místě.

  e) Přidejte tři pravidla, která umožní specifickému uživateli přístup k ADMIN.CHAN jako `MQ-admin` z určitých adres IP:

     – Nastavit hodnotu NOACCESS z libovolné adresy
     – Nastavte parametr BLOCKUSER pro tento kanál na hodnotu pouze blokovat uživatele nobody, což přepíše parametr *MQADMIN BLOCKUSER.
     – POVOLIT přístup k uživateli `mqadm` na určité podsíti adres a oprávnění uživatele MAP k produktu `mqadm`

Chcete-li to provést, spusťte následující příkazy MQSC:

```
SET CHLAUTH (ADMIN.CHAN) TYPE(ADDRESSMAP) ADDRESS('*') USERSRC(NOACCESS)
SET CHLAUTH('ADMIN.CHAN') TYPE(BLOCKUSER) +
DESCR('Rule to override *MQADMIN blockuser on this channel') +
USERLIST('nobody') ACTION(replace)
SET CHLAUTH('ADMIN.CHAN') TYPE(USERMAP) +
CLNTUSER('mqadm') USERSRC(MAP) MCAUSER('mqadm') +
ADDRESS('192.168.1.*') +
DESCR('Allow mqadm as mqadm on local subnet') ACTION(ADD)
```

V tomto bodě může uživatel `mqadm` přistoupit a spustit ADMIN.CHAN z uvedeného rozsahu adres IP.

f) Volitelné: Můžete kdykoli spustit příkaz MQSC MATCH (RUNCHECK), abyste viděli výsledky každého z těchto příkazů:

```
DISPLAY CHLAUTH (ADMIN.CHAN) MATCH (RUNCHECK) CLNTUSER ('mqadm') ADDRESS
('192.168.1.138')
AMQ8878: Display channel authentication record details.
CHLAUTH(ADMIN.CHAN) TYPE(USERMAP)
ADDRESS(192.168.1.*) CLNTUSER(mqadm)
MCAUSER(mqadm)
```

```
DISPLAY CHLAUTH (ADMIN.CHAN) MATCH (RUNCHECK) CLNTUSER ('alice') ADDRESS
('192.168.1.138')
AMQ8878: Display channel authentication record details.
CHLAUTH(ADMIN.CHAN) TYPE(ADDRESSMAP)
ADDRESS(*) USERSRC(NOACCESS)
```

V tomto bodě mají přístup pomocí ADMIN.CHAN.

- **Řízení přístupu pro specifického uživatele a IBM MQ klientskou aplikaci**

  Pro tento scénář jsou výchozí pravidla CHLAUTH přiměřená, za předpokladu, že by pro specifického uživatele mělo být nastaveno oprávnění IBM MQ , aby poskytovala správné oprávnění IBM MQ (pomocí setmqaut).

  V tomto scénáři jsou oprávnění nastavena pro uživatele `mqapp1`, který není uživatelem produktu `MQ-admin` .

  a) Pomocí následujícího příkazu MQSC vytvořte kanál SVRCONN APP1.CHAN, který má být používán konkrétní aplikací a specifickým uživatelem.

```
DEFINE CHANNEL (APP1.CHAN) CHLTYPE (SVRCONN) TRPTYPE (TCP)
```

b) S výchozími pravidly CHLAUTH na místě může uživatel `mqapp1` spustit APP1.CHAN .

ID uživatele přicházející z klientské aplikace IBM MQ se používá pro kontrolu oprávnění k objektu IBM MQ . V tomto případě se za předpokladu, že uživatel `mqapp1` spouští klientskou aplikaci IBM MQ , použije pro kontrolu oprávnění k objektu IBM MQ . Proto, pokud má produkt `mqapp1` přístup k objektům IBM MQ , které aplikace potřebuje, vše je v pořádku; pokud ne, obdržíte chyby oprávnění.

Zabezpečení můžete dále zvýšit vytvořením specifických pravidel CHLAUTH pro ID uživatele `mqapp1` , ale pod výchozími pravidly nemá žádný člen skupiny `MQ-admin` přístup k tomuto kanálu.

Spusťte následující příkazy MQSC:

```
SET CHLAUTH (APP1.CHAN) TYPE(ADDRESSMAP) ADDRESS('*') USERSRC(NOACCESS)
SET CHLAUTH('APP1.CHAN') TYPE(USERMAP) +
CLNTUSER('mqapp1') USERSRC(MAP) MCAUSER('mqapp1') +
DESCR('Allow mqapp1 as mqapp1 on local subnet') ACTION(ADD)
```

- **Řízení přístupu pro specifického uživatele pomocí rozlišujícího názvu (DN) certifikátu tohoto uživatele**

V tomto scénáři musí mít uživatel certifikát, který je protékán do správce front. Rozlišující název je pak porovnán s nastavením SSLPEER pravidla CHLAUTH a SSLPEER může používat zástupné znaky.

Pokud se shoduje, může být uživatel také mapován na jiného uživatele MCAUSER pro účely kontroly oprávnění k objektu IBM MQ . Mapování uživatele MCAUSER může minimalizovat počet uživatelů, které je třeba spravovat ve správci OAM (Object Authority Manager) systému IBM MQ .

a) Máte kanál TLS s používanými certifikáty a vyžadujete pravidla pro:

   – Blokovat všechny uživatele pro konkrétní kanál
   – Povolte pouze uživatele s konkrétním SSLPEER, kteří používají klienta tohoto uživatele pro přístup k produktu IBM MQ OAM.

   Spusťte následující příkazy MQSC:

```
.
# block all users on any IP address.
SET CHLAUTH('SSL1.SVRCONN') TYPE(ADDRESSMAP) ADDRESS('*')
USERSRC(NOACCESS) DESCR(''block all'') WARN(NO) ACTION(ADD)
.
# override - no MQM admin rule (allow mqm group /mqm admin users to
connect.
SET CHLAUTH('SSL1.SVRCONN') TYPE(BLOCKUSER) USERLIST('nobody')
DESCR('override no mqm admin rule') WARN(NO) ACTION(ADD)
.
# allow particular SSLPEER, use client id coming in from channel
SET CHLAUTH('SSL1.SVRCONN') TYPE(SSLPEERMAP)
SSLPEER('CN=JOHNDOE,O=IBM,C=US') USERSRC(CHANNEL) ACTION(ADD)
```

   ID uživatele klienta, který se připojuje ke kanálu, se používá pro oprávnění IBM MQ OAM objektů IBM MQ ; proto musí mít ID uživatele odpovídající oprávnění IBM MQ .

b) Volitelné: Namapujte na jiné ID uživatele IBM MQ .

   Znovu spusťte předchozí příkaz MQSC a nahraďte USERSRC(MAP) MCAUSER('mquser1') za USERSRC(CHANNEL).

- **Mapovat konkrétního uživatele na `mqm` uživatele**

  Jedná se o přidání nebo úpravu volby Řízení přístupu pro specifické uživatele MQ-admin.

  Pomocí příkazů MQSC přidejte následující pravidlo CHLAUTH k mapování konkrétních uživatelů na uživatele `mqm` nebo ID uživatele `MQ-admin` , který má nastavení oprávnění k objektu IBM MQ v produktu IBM MQ OAM.

```
SET CHLAUTH('ADMIN.CHAN') TYPE(USERMAP) +
CLNTUSER ('johndoe') USERSRC(MAP) MCAUSER ('mqm') +
ADDRESS('192.168.1-100.*') +
DESCR ('Allow johndoe as MQ-admin on local subnet') ACTION (ADD)
```

  To umožňuje a mapuje uživatele `johndoe` na uživatele `mqm` pro konkrétní kanál ADMIN.CHAN.

Související pojmy

“Vytváření nových pravidel CHLAUTH pro kanály” na stránce 66
Chcete-li vám pomoci vytvořit vlastní pravidla CHLAUTH, zde jsou některé běžné scénáře pro kanály a příklad pravidel CHLAUTH k jejich dosažení.

Související úlohy

“Řešení problémů s přístupem CHLAUTH” na stránce 62
Kroky a příklady k vyřešení určitých problémů s přístupem při použití záznamů ověření kanálu (CHLAUTH).

Související odkazy

NASTAVIT CHLAUTH
ZOBRAZITYCHLAUTH

Vytváření nových pravidel CHLAUTH pro kanály

Chcete-li vám pomoci vytvořit vlastní pravidla CHLAUTH, zde jsou některé běžné scénáře pro kanály a příklad pravidel CHLAUTH k jejich dosažení.

Toto téma obsahuje následující scénáře:

- “Povolit přístup ke konkrétnímu kanálu pouze z určitého rozsahu adres IP.” na stránce 67
- “Pro specifický kanál zablokujte všechny uživatele, ale povolte připojení specifických uživatelů.” na stránce 67
- “Použití CHLAUTH pro kanály přijímače a odesílatele” na stránce 68

Povolit přístup ke konkrétnímu kanálu pouze z určitého rozsahu adres IP.

Pro tento scénář chcete:

- Nenastavte žádný přístup ke kanálu odkudkoli
- Povolit přístup z určité adresy IP nebo rozsahu adres

```
runmqsc:
SET CHLAUTH('APP2.CHAN') TYPE(ADDRESSMAP) ADDRESS('*') USERSRC(NOACCESS)
WARN(NO) ACTION(ADD)
SET CHLAUTH('APP2.CHAN') TYPE(ADDRESSMAP) ADDRESS('9.95.100.1-5')
USERSRC(MAP) MCAUSER('mqapp2') ACTION(ADD)
```

To umožňuje pouze APP2.CHAN , který se má spustit, když připojení přichází z uvedeného rozsahu adres IP.

Uživatel, který se připojuje jako MCAUSER, je namapován na `mqapp2`, a proto získá oprávnění IBM MQ OAM pro tohoto uživatele.

Pro specifický kanál zablokujte všechny uživatele, ale povolte připojení specifických uživatelů.

Pro zpracování CHLAUTH existují tři výchozí pravidla:

- ŽÁDNÝ PŘÍSTUP KE VŠEM KANÁLŮM ZE STRANY UŽIVATELŮ `MQ-admin*`
- ŽÁDNÝ PŘÍSTUP KE VŠEM SYSTÉMŮM. * kanály všech uživatelů
- POVOLIT přístup k SYSTEM.ADMIN.SVRCONN (bez uživatelů `MQ-admin`)

První dvě pravidla blokují přístup ke všem kanálům. Třetí pravidlo je specifičtější, a proto má přednost před ostatními dvěma, pokud je kanál SYSTEM.ADMIN.SVRCONN umožňuje přístup k tomuto kanálu.

Pro tento scénář má přístup ke kanálu MY.SVRCONN výchozí pravidla CHLAUTH.

Musíte přidat následující:

```
# block all users
SET CHLAUTH('MY.SVRCONN') TYPE(ADDRESSMAP) ADDRESS('*') USERSRC(NOACCESS)
DESCR(''block all'') WARN(NO) ACTION(ADD)

# override - no MQM admin rule
SET CHLAUTH('MY.SVRCONN') TYPE(BLOCKUSER) USERLIST('nobody') DESCR('override
no mqm admin rule') WARN(NO) ACTION(ADD)

# allow johndoe userid
SET CHLAUTH('MY.SVRCONN') TYPE(USERMAP) CLNTUSER('johndoe')
USERSRC(CHANNEL) DESCR('allow johndoe userid') ACTION(ADD)
```

Tato první část kódu blokuje, aby se kdokoli připojil na MY.SVRCONN, pak kód umožňuje, aby byl spuštěn pouze kanál MY.SVRCONN , když připojení pochází ze specifického ID uživatele `johndoe`.

Uživatel, který se připojuje ke kanálu `johndoe` , se používá pro oprávnění IBM MQ OAM objektů IBM MQ . Proto musí mít ID uživatele odpovídající oprávnění IBM MQ .

Pokud chcete, můžete provést mapování na jiné ID uživatele produktu IBM MQ pomocí:

```
USERSRC(MAP) MCAUSER('mquser1')
```

místo USERSRC(CHANNEL).

Použití CHLAUTH pro kanály přijímače a odesílatele

Pomocí pravidel CHLAUTH můžete přidat další zabezpečení pro kanály příjemce a odesílatele, abyste omezili přístup k kanálu příjemce. Všimněte si, že pokud přidáváte nebo měníte pravidla CHLAUTH, platí aktualizovaná pravidla CHLAUTH pouze při spuštění kanálu, takže pokud jsou kanály již spuštěny, musíte je zastavit a restartovat, aby se použily aktualizace CHLAUTH.

Pravidla CHLAUTH lze použít na libovolném kanálu, ale existují určitá omezení. Například pravidla USERMAP platí pouze pro kanály SVRCONN.

Tento příklad umožňuje připojení pouze z konkrétní adresy IP ke spuštění TO.MYSVR1 :

```
# First you could lock down the channel by disallowing all
# for channel 'TO.MYSVR1', RCVR channel
SET CHLAUTH('TO.MYSVR1') TYPE(ADDRESSMAP) ADDRESS('*') USERSRC(NOACCESS)
DESCR('Back-stop rule')

# Then you could allow this channel to be started
SET CHLAUTH('TO.MYSVR1') TYPE(ADDRESSMAP) ADDRESS('192.168.1.134') USERSRC(MAP)
MCAUSER('mqapp') ACTION(ADD)
```

Tento příklad umožňuje připojení pouze z konkrétního správce front:

```
# Lock down all access:
SET CHLAUTH('TO.MYSVR1') TYPE(ADDRESSMAP) ADDRESS('*') USERSRC(NOACCESS)
DESCR('Back-stop rule')

# Then allow access from queue manager MYSVR2 and from a particular ipaddress:
SET CHLAUTH('TO.MYSVR1') TYPE(QMGRMAP) QMNAME('MYSVR2') USERSRC(MAP)
MCAUSER('mqapp') ADDRESS('192.168.1.134') ACTION(ADD)
```

Související úlohy

“Řešení problémů s přístupem CHLAUTH” na stránce 62
Kroky a příklady k vyřešení určitých problémů s přístupem při použití záznamů ověření kanálu (CHLAUTH).

“Vytvoření nových pravidel CHLAUTH pro uživatele” na stránce 64
Některé běžné scénáře pro uživatele a příklad pravidel CHLAUTH k jejich provedení.

Související odkazy

NASTAVIT CHLAUTH

ZOBRAZITYCHLAUTH

Vytvoření pravidla back-stop CHLAUTH

Při přemýšlení o řízení příchozích připojení do správce front máte dvě možnosti. Buď se můžete pokusit vypsat všechna připojení, která nejsou povolena, nebo můžete začít tím, že řeknete, že všechna připojení nejsou povolena, a pak se pokusíte vypsat všechna připojení, která jsou povolena. Tato druhá možnost je popsána zde.

Informace o této úloze

Důvodem pro použití druhé volby je, že pokud se pokusíte vypsat všechna připojení, která nejsou povolena, a vše, co není uvedeno, je povoleno v seznamu, výsledkem chybějícího jednoho ze seznamu je, že připojení, které nemělo být povoleno, se může připojit, což způsobí potenciální narušení zabezpečení.

Naopak, pokud místo toho začnete tím, že každé připojení není povoleno, a pak vypište ty, které jsou, výsledek chybějícího jednoho z tohoto seznamu není narušení zabezpečení. Pokud váš podnik vyžaduje přidání dalších připojení, jedná se o poměrně jednoduchou úlohu, ale nedochází k potenciálnímu narušení zabezpečení.

První věcí, kterou je třeba udělat, je vytvořit pravidlo *back-stop* , což je pravidlo, které zachytí všechna připojení, která se jinak neshodují s konkrétnějšími pravidly. Toto pravidlo má za následek zastavení všech vzdálených připojení, aby se vůbec mohla připojit ke správci front.

Pokud vás však tento přístup znepokojuje, můžete nastavit pravidlo *back-stop* v režimu varování; viz krok “2” na stránce 69 .

Postup

1. Chcete-li vytvořit pravidlo back-stop, které zastaví vzdálená připojení připojená ke správci front, zadejte následující příkaz:

   ```
   SET CHLAUTH('*') TYPE(ADDRESSMAP) ADDRESS('*')
   USERSRC(NOACCESS) DESCR('Back-stop rule')
   ```

   Nyní, když jste zavřeli dveře na všech vzdálených připojeních, můžete začít používat konkrétnější pravidla, která umožní určitá připojení. Příklad:

   ```
   SET CHLAUTH('APPL1.SVRCONN') TYPE(ADDRESSMAP) ADDRESS('9.20.1-3.*') USERSRC(CHANNEL)
   SET CHLAUTH('SYSTEM.ADMIN.*') TYPE(SSLPEERMAP) SSLPEER('O=IBM') USERSRC(CHANNEL)
   SET CHLAUTH('TO.QM2') TYPE(QMGRMAP) QMNAME('QM1') USERSRC(MAP) MCAUSER('QM1USER')
   SET CHLAUTH('*.SVRCONN') TYPE(USERMAP) CLNTUSER('johndoe') MCAUSER('johndoe@yourdomain')
   SET CHLAUTH('*') TYPE(SSLPEERMAP) SSLPEER('CN="John Doe"') ADDRESS('9.*') MCAUSER('johndoe')
   ```

2. Chcete-li vytvořit pravidlo back-stop v režimu varování, zadejte následující příkaz:

   ```
   SET CHLAUTH('*') TYPE(ADDRESSMAP) ADDRESS('*')
   USERSRC(NOACCESS) DESCR('Back-stop rule') WARN(YES)
   ```

   Nyní můžete pokračovat a vytvořit všechna vaše pozitivní pravidla. Pokud se domníváte, že jste vytvořili všechna pravidla, která potřebujete, zapněte události kanálu zadáním následujícího příkazu:

   ```
   ALTER QMGR CHLEV(EXCEPTION)
   ```

   a monitorujte SYSTEM.ADMIN.CHANNEL.EVENT pro události s hodnotou **Reason** nastavenou na MQRC_CHANNEL_BLOCKED_WARNING.

   Tyto události podrobně popisují připojení, která odpovídají vašemu pravidlu back-stop, ale protože příkaz běží v režimu varování, nebyly momentálně blokovány.

   Přezkoumejte každou z těchto událostí a určete, zda by toto připojení mělo mít kladné pravidlo, které by jej povolilo, nebo zda bylo správně porovnáno s pravidlem *back-stop* . Můžete spustit v tomto režimu, zkontrolovat události, jak jsou vytvořeny, dokud nejste rádi, že jste viděli všechny příchozí kanály, a mít odpovídající pozitivní pravidla pro všechny.

   V tomto bodě můžete změnit pravidlo *back-stop* tak, aby spustilo skutečně blokující připojení, která odpovídají, zadáním následujícího příkazu:

   ```
   SET CHLAUTH('*') TYPE(ADDRESSMAP) ADDRESS('*')
   USERSRC(NOACCESS) DESCR('Back-stop rule') WARN(NO)
   ACTION(REPLACE)
   ```

Vytvoření neprivilegovaného administrátora IBM MQ
Jak vytvoříte neprivilegovaného administrátora produktu IBM MQ pomocí CHLAUTH.

Informace o této úloze

V kontextu této úlohy se jedná o tyto pojmy:

oprávněný uživatel
Znamená uživatele, který má oprávnění k provedení operace, aniž by mu byl výslovně udělen přístup k provedení této operace. Uživatelé ve skupině mqm jsou příklady těchto oprávněných uživatelů.

IBM MQ administrátor
Znamená uživatele, který potřebuje zadat administrativní příkazy pro systém IBM MQ, například **DEFINE QLOCAL** nebo **START CHANNEL**.

Následující kroky vytvoří neprivilegovaného administrátora produktu IBM MQ .

Postup

1. Vytvořte ID uživatele v počítači správce front pomocí příslušných příkazů pro platformu nebo platformy, které váš podnik používá.

   V tomto příkladu se používá jméno uživatele `alice` .
2. Udělte tomuto novému uživateli oprávnění k vydávání všech administrativních příkazů IBM MQ provedením následujícího postupu:
   a) Spusťte IBM MQ Explorer pomocí privilegovaného uživatele.
   b) Přejděte do *Průvodce na základě rolí* výběrem příslušného správce front, poté `Oprávnění objektů` a `Přidat oprávnění na základě rolí`.
   c) Na panelu průvodce, který se objeví, zadejte ID uživatele, které jste vytvořili v prvním kroku, nebo pokud dáváte přednost práci se skupinami, zadejte název skupiny pro uživatele nebo sadu uživatelů, které chcete vytvořit pro neprivilegované administrátory produktu IBM MQ .
   d) Nastavte průvodce pro úplný administrativní přístup.
   e) Chcete-li administrátorovi systému IBM MQ bez oprávnění povolit procházení zpráv ve frontách, zaškrtněte toto políčko.
   f) Zkontrolujte příkazy na panelu náhledu v dolní části průvodce.

      Tyto příkazy můžete vyjmout a vložit, abyste vytvořili vlastní skripty.

      Jedním z důvodů, proč byste to mohli raději dělat s vlastním skriptem, je snížit množství přístupu, který tomuto uživateli poskytnete. Spíše než abyste udělili přístup ke všem objektům, můžete raději udělit přístup pouze určité skupině objektů.

      Stisknutí tlačítka **OK** v průvodci vydá příkazy tak, jak jsou zobrazeny.
   g) Musíte nastavit některá pravidla CHLAUTH, abyste povolili vzdálený přístup pro toto ID uživatele, pokud má být požadavek na neprivilegovaného administrátora produktu IBM MQ také pro vzdálený přístup.

      Za předpokladu, že váš podnik používá pokyny v části “Vytvoření pravidla back-stop CHLAUTH” na stránce 68, vše, co musíte udělat, je přidat aktivační pravidlo.

      Pravidlo, které vytvoříte, závisí spíše na tom, jak se rozhodnete ověřit vzdálené administrátory produktu IBM MQ .

      Pokud používáte slabé ověření TCP/IP, můžete nastavit pravidlo CHLAUTH, které vypadá takto:

      ```
        SET CHLAUTH(admin-channel-name)      TYPE(ADDRESSMAP)
      ADDRESS('1.2.3.4')      USERSRC(MAP) MCAUSER('alice')
      DESCR('Admin Channel - Weak TCP/IP authentication')
      ```

      9. Pokud používáte ověření TLS, můžete nastavit pravidlo CHLAUTH, které vypadá takto:

      ```
      SET CHLAUTH(admin-channel-name)      TYPE(SSLPEERMAP)
      SSLPEER('CN=Alice') ADDRESS('1.2.3.4')      USERSRC(MAP) MCAUSER('alice')
      DESCR('Admin Channel - TLS authentication'
      ```

      Nyní, když se uživatel připojí k serveru `admin-channel-name` (a odpovídá pravidlům CHLAUTH), může zadat příkazy pod ID uživatele `alice` ve správci front, a proto není vyžadován oprávněný vzdálený přístup.

Ověření připojení

Ověřování připojení umožňuje aplikacím při připojení ke správci front zadávat ověřovací pověření. Správce front ověřuje pověření. ID uživatele zadané v pověřeních lze také přijmout pro použití při kontrolách autorizace pro prostředky, ke kterým aplikace přistupuje.

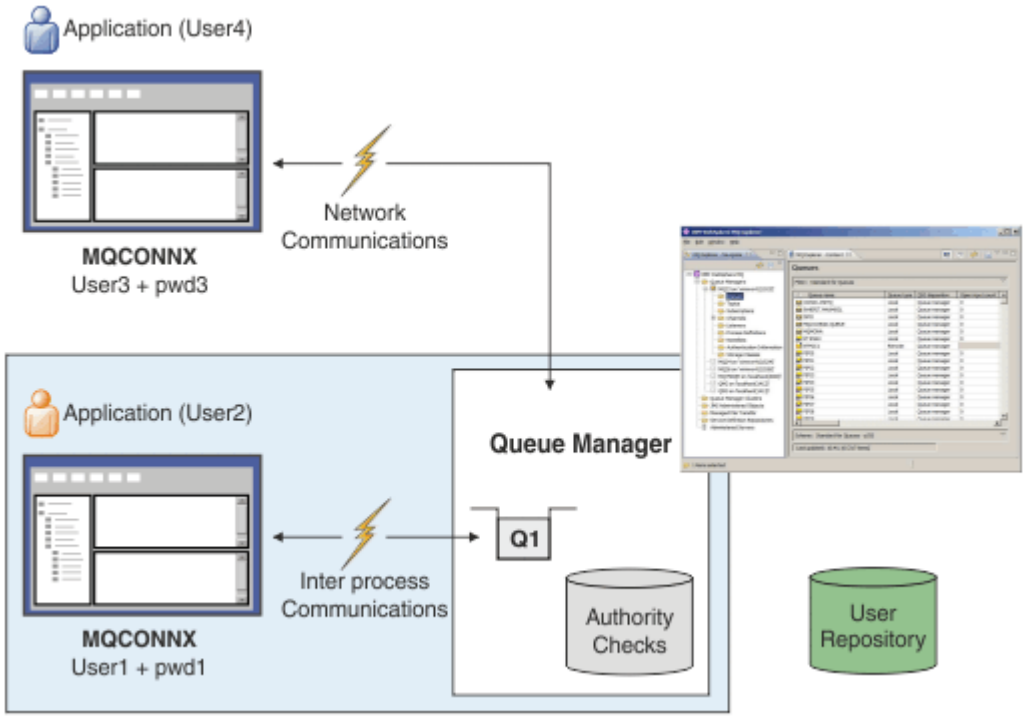
Aplikace mohou při připojení ke správci front zadat ID uživatele a heslo pro ověření.

V 9.3.4 V produktu IBM MQ 9.3.4mohou aplikace produktu IBM MQ client také dodat token ověření jako alternativní metodu ověření.

Správce front lze konfigurovat tak, aby ověřoval pověření dodaná aplikací.

ID uživatele a heslo dodané aplikací je kontrolováno pomocí úložiště uživatelů v konfiguraci správce front. Další informace o úložišti, které se používá pro kontrolu ID uživatelů a hesel, naleznete v tématu Úložiště uživatelů.

V 9.3.4 Tokeny ověřování jsou ověřovány pomocí certifikátů a symetrických klíčů v úložišti klíčů ověřování tokenů správce front za účelem ověření podpisu tokenu. Další informace o ověřování uživatelů pomocí tokenů ověření viz “Práce s tokeny ověření” na stránce 349.



V diagramu dvě aplikace navazují připojení se správcem front, jedna aplikace jako klient a jedna s použitím lokálních vazeb. Aplikace mohou pro připojení ke správci front používat různá rozhraní API, ale všechny mají možnost zadat ID uživatele a heslo. ID uživatele, pod kterým je aplikace spuštěna, `User2` a `User4` v diagramu, což je obvyklé ID uživatele operačního systému prezentované produktu IBM MQ, se může lišit od ID uživatele poskytnutého aplikací `User1` a `User3`.

Správce front přijímá konfigurační příkazy (v diagramu se používá IBM MQ Explorer) a spravuje otevírání prostředků a kontroluje oprávnění pro přístup k těmto prostředkům. V produktu IBM MQ existuje mnoho různých prostředků, ke kterým může aplikace vyžadovat oprávnění pro přístup. Diagram ilustruje otevření fronty pro výstup, ale stejné zásady platí i pro ostatní prostředky.

Související pojmy

“Ověření připojení: Konfigurace” na stránce 71
Správce front lze nakonfigurovat tak, aby ověřoval pověření dodaná aplikací při připojení.

“Ověření připojení: Změny aplikace” na stránce 76

“Ověření připojení: Úložiště uživatelů” na stránce 77
Pro každého z vašich správců front můžete zvolit různé typy objektů ověřovacích informací pro ověřování ID uživatelů a hesel.

Ověření připojení: Konfigurace

Správce front lze nakonfigurovat tak, aby ověřoval pověření dodaná aplikací při připojení.

Zapnutí ověřování připojení ve správci front

V objektu správce front lze atribut **CONNAUTH** nastavit na název objektu ověřovacích informací (AUTHINFO). Atribut **AUTHTYPE** objektu AUTHINFO určuje typ objektu. Objekty AUTHINFO, které se používají pro ověření připojení, mohou být jednoho z následujících dvou typů:

IDPWOS
Správce front používá lokální operační systém k ověření ID uživatele a hesla dodaného připojující se aplikací.

V systému IBM MQ 9.3.4tento typ objektu AUTHINFO také umožňuje správci front, který je spuštěn v operačním systému AIX nebo Linux , ověřit tokeny ověření. Kromě objektu AUTHINFO, který se používá ke konfiguraci ověření připojení, musí být správce front nakonfigurován tak, aby přijímal tokeny ověření s sekcí **AuthInfo** souboru `qm.ini` . Další informace o konfiguraci správce front pro přijímání tokenů ověřování naleznete v tématu “Konfigurace správce front pro přijetí tokenů ověřování” na stránce 353.

IDPWLDAP
Správce front používá server LDAP k ověření ID uživatele a hesla dodaného připojující se aplikací.

Poznámka: Do atributu **CONNAUTH** správce front nelze zadat žádný jiný typ objektu ověřovacích informací.

Objekty AUTHINFO typu `IDPWOS` a `IDPWLDAP` jsou podobné v několika svých atributech. Zde popsané atributy jsou společné pro oba typy objektů.

Následující příklad příkazů MQSC zapne ověřování připojení pomocí následujících operací:

1. Definujte objekt AUTHINFO s názvem `USE.PW`.
2. Změňte atribut **CONNAUTH** správce front tak, aby odkazoval na tento objekt AUTHINFO.
3. Zadáním příkazu **REFRESH SECURITY** aktualizujte konfiguraci ověřování připojení správce front. Příkaz **REFRESH SECURITY** musí být zadán dříve, než správce front rozpozná všechny změny v konfiguraci ověřování připojení.

```
DEFINE AUTHINFO(USE.PW) +
AUTHTYPE(IDPWOS) +
FAILDLAY(10) +
CHCKLOCL(OPTIONAL) +
CHCKCLNT(REQUIRED)

ALTER QMGR CONNAUTH(USE.PW)

REFRESH SECURITY TYPE(CONNAUTH)
```

Chcete-li řídit, zda jsou kontrolována pověření pro připojení, která jsou vytvořena lokálně vázanými aplikacemi, použijte atribut AUTHINFO **CHCKLOCL** (zkontrolujte lokální připojení). Chcete-li řídit, zda jsou kontrolována pověření pro připojení vytvářená klientskými aplikacemi, použijte atribut AUTHINFO **CHCKCLNT** (zkontrolujte připojení klienta).

CHCKLOCL přijímá hodnoty `NONE` a `OPTIONAL`a **CHCKCLNT** umožňuje konfigurovat hodnotu `NONE` pro požadavky na ověření:

NONE
Ověřovací pověření, která jsou dodána aplikacemi, nejsou kontrolována.

Volitelný
Zajišťuje, že všechna pověření poskytnutá aplikací jsou platná. Není však povinné, aby aplikace poskytovaly ověřovací pověření. Tato volba může být užitečná například během migrace.

Pokud jste:

- Zadejte jméno uživatele a heslo, jsou ověřeny.
- Nezadávejte jméno uživatele a heslo, připojení je povoleno.
- Zadejte jméno uživatele, ale ne heslo, na které jste obdrželi chybu.

Důležité: `VOLITELNĚ` je minimální hodnota, kterou můžete nastavit, chcete-li také nastavit více omezující volbu v pravidlech ověření kanálu (CHLAUTH).

Pokud vyberete volbu NONE a připojení klienta odpovídá záznamu CHLAUTH s hodnotou **CHCKCLNT** nastavenou na REQUIRED (nebo REQDADM na jiných platformách než z/OS), připojení se nezdaří. Obdržíte zprávu AMQ9793 na jiných platformách než z/OSa zprávu CSQX793E na systému z/OS.

Další informace o použití pravidel ověřování kanálu k nastavení více omezujících voleb **CHCKCLNT** pro některá připojení klienta naleznete v části "Granularita konfigurace" na stránce 73.

POVINNÉ
Vyžaduje, aby všechny aplikace poskytovaly platná pověření. Viz také následující poznámka.

REQDADM
Oprávnění uživatelé musí zadat platná pověření, ale s neprivilegovanými uživateli se zachází jako s nastavením OPTIONAL . Viz také následující poznámka. z/OS (Toto nastavení není v systémech z/OS povoleno.)

Poznámka:

Nastavení parametru **CHCKLOCL** na hodnotu REQUIRED nebo REQDADM znamená, že správce front nelze lokálně spravovat pomocí příkazu **runmqsc** (chyba AMQ8135: Neautorizováno), pokud uživatel nezadá parametr **-u** pro zadání ID uživatele v příkazu **runmqsc** . Při nastavení tohoto parametru produkt **runmqsc** zobrazí výzvu k zadání hesla uživatele v konzole.

Podobně se uživateli, který spouští produkt IBM MQ Explorer v lokálním systému, při pokusu o připojení ke správci front zobrazí chyba AMQ4036 . Chcete-li zadat ID uživatele a heslo, klepněte pravým tlačítkem myši na objekt lokálního správce front a vyberte volbu **Podrobnosti připojení** > **Vlastnosti ...** z nabídky. V sekci **ID uživatele** zadejte ID uživatele a heslo, které se má použít, a poté klepněte na tlačítko **OK**.

Podobné pokyny platí pro vzdálená připojení s produktem **CHCKCLNT**.

Atribut **CONNAUTH** správce front je prázdný pro správce front, kteří jsou migrováni ze starších verzí než IBM MQ 8.0, ale je nastaven na hodnotu *SYSTEM.DEFAULT.AUTHINFO.IDPWOS* pro nově vytvořené správce front. Tato výchozí definice **AUTHINFO** má standardně nastavenu hodnotu **CHCKCLNT** REQDADM .

Proto musí existující klienti, kteří pro připojení používají ID oprávněného uživatele, poskytnout platná pověření.

Varování: Pověření ve struktuře MQCSP pro klientskou aplikaci jsou někdy odesílána po síti jako prostý text. Chcete-li se ujistit, že jsou pověření klienta chráněná, prohlédněte si téma "Ochrana heslem MQCSP" na stránce 31.

Granularita konfigurace

Atributy **CHCKLOCL** a **CHCKCLNT** objektu AUTHINFO nastavují požadavky na ověření pro všechna připojení ke správci front. Kromě těchto atributů umožňují pravidla atributu **CHCKCLNT** na ověření kanálu (CHLAUTH) nastavit přísnější požadavky na ověření pro specifická připojení klienta, která odpovídají pravidlu CHLAUTH.

Celkovou hodnotu **CHCKCLNT** můžete nastavit na OPTIONAL, například v objektu AUTHINFO, a poté ji upgradovat na přísnější nastavení pro určité kanály nastavením **CHCKCLNT** na hodnotu REQUIRED nebo REQDADM v pravidle CHLAUTH. Standardně jsou pravidla CHLAUTH definována s hodnotou **CHCKCLNT(ASQMGR)**, takže tuto granularitu není nutné použít. Tyto příkazy MQSC například definují jedno pravidlo CHLAUTH, které potlačí atribut **CHCKCLNT** objektu AUTHINFO, a jedno pravidlo CHLAUTH, které nemá:

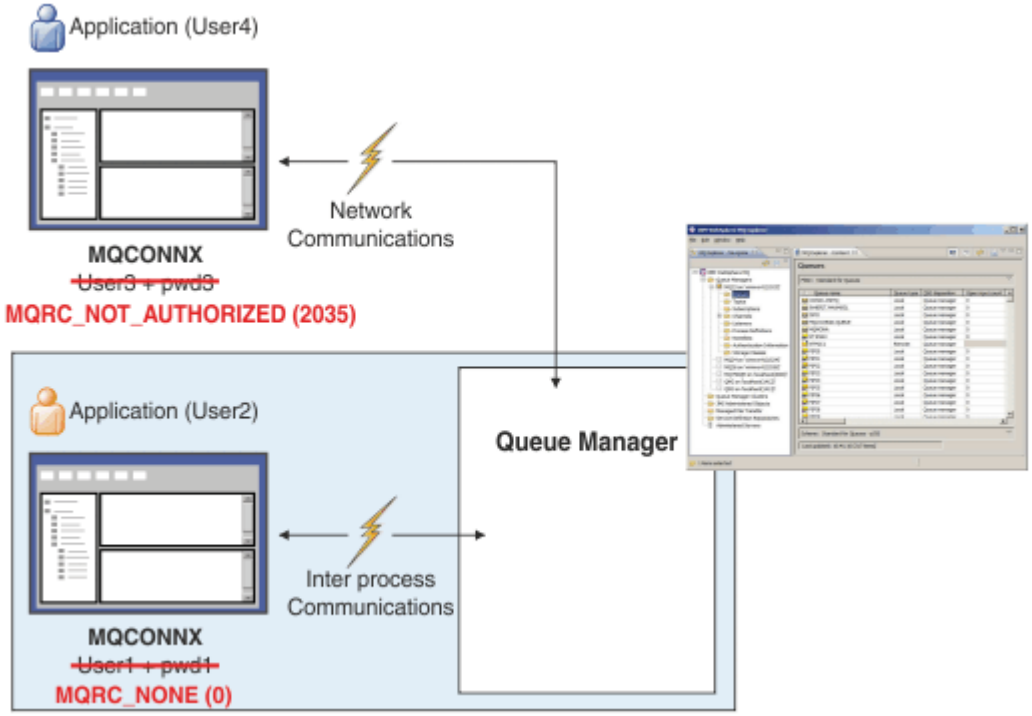
```
DEFINE AUTHINFO(USE.PW) AUTHTYPE(xxxxxx) +
CHCKCLNT(OPTIONAL)

SET CHLAUTH('*') TYPE(ADDRESSMAP) +
ADDRESS('*') USERSRC(CHANNEL) +
CHCKCLNT(REQUIRED)

SET CHLAUTH('*') TYPE(SSLPEERMAP) +
SSLPEER('CN=*') USERSRC(CHANNEL)
```

Další informace o pravidlech CHLAUTH viz "Záznamy ověření kanálu" na stránce 51.

Oznámení o chybě



Chyba je zaznamenána v následujících situacích:

- Aplikace nedodává ověřovací pověření, jsou-li požadována.
- Aplikace poskytuje neplatná ověřovací pověření. Tato situace je považována za chybu, i když konfigurace uvádí, že je pro aplikace volitelné, aby dodaly pověření.

Poznámka: Je-li parametr **CHCKLOCL** nebo **CHCKCLNT** nastaven na hodnotu NONE, nejsou zjištěna neplatná pověření dodaná aplikacemi.

Nezdařená ověření jsou zadržena po dobu v sekundách určenou atributem **FAILDLAY** , než je chyba vrácena aplikaci. Tato prodleva poskytuje určitou ochranu před opakovaným pokusem o připojení aplikace.

Chyba se zaznamenává několika způsoby:

Aplikace
Aplikaci je vrácen kód příčiny MQRC_NOT_AUTHORIZED (2035).

Administrátor
Administrátor systému IBM MQ vidí událost nahlášenou v protokolu chyb. Chybová zpráva ukazuje, že připojení je odmítnuto, protože pověření jsou neplatná, a nikoli například proto, že uživatel nemá oprávnění k připojení.

Nástroj pro monitorování
Nástroj monitorování může být také upozorněn na selhání, pokud zapnete události oprávnění, pomocí zprávy události ve frontě SYSTEM.ADMIN.QMGR.EVENT . Chcete-li zapnout události oprávnění, zadejte následující příkaz MQSC:

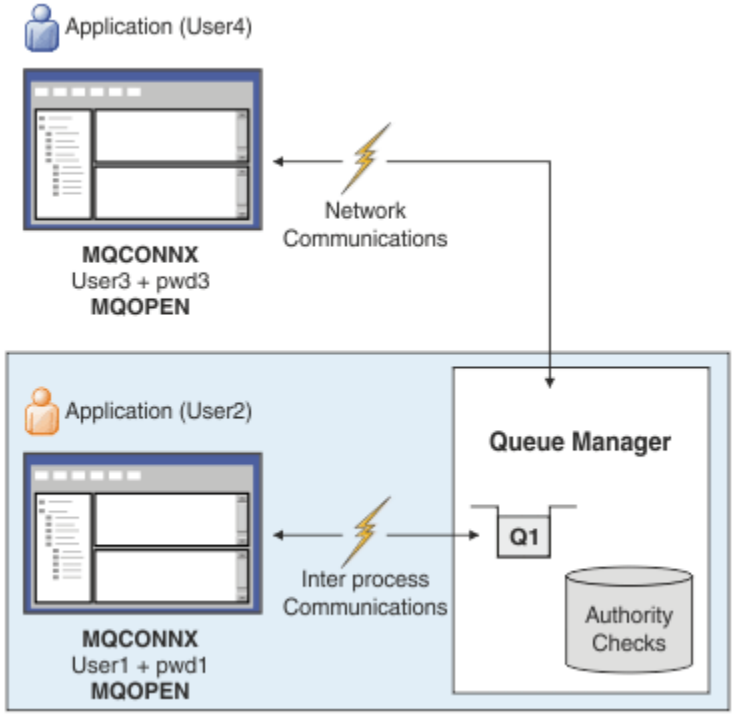
```
ALTER QMGR AUTHOREV(ENABLED)
```

Tato událost "Bez autorizace" je událostí připojení typu 1 a poskytuje stejná pole jako ostatní události typu 1 s dalším polem, které bylo poskytnuto ID uživatele MQCSP. Pokud aplikace zadala heslo, nebude zahrnuto do zprávy události. To znamená, že ve zprávě události jsou dvě ID uživatelů:

- ID uživatele, pod kterým je aplikace spuštěna.
- ID uživatele v pověřeních, která aplikace představila.

Další informace o této zprávě události viz Bez autorizace (typ 1).

Adoptování uživatelů pro autorizaci



Správce front můžete nakonfigurovat tak, aby převzal pověření, která aplikace prezentuje jako kontext pro připojení. Adoptování pověření znamená, že ID uživatele zadané v ověřovacích pověřeních se použije pro kontroly autorizace, zobrazí se na administrativních obrazovkách a objeví se ve zprávách. Atribut **ADOPTCTX** v objektu AUTHINFO řídí, zda jsou pověření převzata jako kontext pro aplikaci. Například následující příkazy MQSC definují objekt AUTHINFO s názvem USE.PWD , který se používá pro ověření připojení, a nastaví atribut **ADOPTCTX** na hodnotu YES:

```
DEFINE AUTHINFO(USE.PWD) +
AUTHTYPE(xxxxxx) +
CHCKLOCL(OPTIONAL) +
CHCKCLNT(REQUIRED) +
ADOPTCTX(YES)

ALTER QMGR CONNAUTH(USE.PWD)
```

Pro atribut **ADOPTCTX** lze zadat následující hodnoty:

POKUD CTX (ANO)
Pověření dodaná aplikací jsou převzata jako kontext aplikace po dobu trvání připojení. Všechny kontroly autorizace pro aplikaci jsou provedeny s ID uživatele v ověřených pověřeních.

Upozornění: Používáte-li produkt **ADOPTCTX(YES)** a ID uživatelů lokálního operačního systému, musíte se ujistit, že adoptované ID uživatele splňuje požadavky na ID uživatelů v produktu IBM MQ. Další informace viz téma “ID uživatelů” na stránce 88.

ADOPTCTX (NO)
Pověření dodaná aplikací se používají pouze pro ověření v době připojení. ID uživatele, pod kterým je aplikace spuštěna, se nadále používá pro budoucí kontroly autorizace. Tato volba může být užitečná při migraci nebo pokud plánujete použít jiné mechanizmy, například záznamy ověření kanálu, k přiřazení identifikátoru uživatele agenta kanálu zpráv (MCAUSER).

Interakce s ověřením kanálu

Pravidla ověřování kanálu lze použít ke změně ID uživatele, které se používá jako kontext pro připojení aplikace, na základě ID uživatele přijatého od klienta. Příklad použití pravidla ověřování kanálu ke změně ID uživatele přidruženého k připojení viz “Mapování ID uživatele klienta na ID uživatele MCAUSER” na stránce 406.

Pořadí, ve kterém jsou pravidla ověřování připojení a ověřování kanálu zpracována, je významným faktorem při určování kontextu zabezpečení pro připojení klientských aplikací IBM MQ . Parametr **ChlauthEarlyAdopt** v sekci **channels** souboru `qm.ini` řídí pořadí, ve kterém správce front převezme kontext z pověření dodaných aplikací, a použije pravidla ověřování kanálu. Další informace o produktu **ChlauthEarlyAdopt**naleznete v tématu Atributy sekce kanálů.

Upozornění: Když použijete parametr **ADOPTCTX(YES)** na objektu ověřovacích informací, kontext, který je převzat z pověření dodaných aplikací, lze změnit pomocí pravidel ověřování kanálu pouze v případě, že je parametr **ChlauthEarlyAdopt** nastaven na hodnotu Y.

Další informace o interakci ověřování připojení a ověřování kanálu a pořadí, ve kterém se kontroly provádějí při připojení klientské aplikace ke správci front, naleznete v části “Interakce CHLAUTH a CONNAUTH” na stránce 57.

Související pojmy

“Ověření připojení” na stránce 70
Ověřování připojení umožňuje aplikacím při připojení ke správci front zadávat ověřovací pověření. Správce front ověřuje pověření. ID uživatele zadané v pověřeních lze také přijmout pro použití při kontrolách autorizace pro prostředky, ke kterým aplikace přistupuje.

“Ověření připojení: Změny aplikace” na stránce 76

“Ověření připojení: Úložiště uživatelů” na stránce 77
Pro každého z vašich správců front můžete zvolit různé typy objektů ověřovacích informací pro ověřování ID uživatelů a hesel.

Ověření připojení: Změny aplikace

Aplikace, která používá rozhraní fronty zpráv (MQI), může poskytnout ID uživatele a heslo ve struktuře parametrů zabezpečení připojení (MQCSP) při volání MQCONNX. V jiných rozhraních API je struktura MQCSP obvykle sestavena za aplikaci knihovnami IBM MQ .

V 9.3.4 Z produktu IBM MQ 9.3.4mohou klientské aplikace, které se připojují ke správci front spuštěnému v systémech AIX nebo Linux , také odeslat token ověření ve struktuře MQCSP jako alternativní způsob identifikace.

ID uživatele a heslonebo token ověření jsou předány ke kontrole správci oprávnění k objektu (OAM) dodanému se správcem front nebo komponentě služby autorizace dodávané se správcem front v systémech z/OS . Nemusíte psát své vlastní rozhraní.

Je-li aplikace spuštěna jako klient, ID uživatele a heslonebo token ověření, předá se produkt také uživatelským procedur zabezpečení na straně klienta a serveru pro zpracování. Lze je také použít k nastavení atributu MCAUSER (identifikátor uživatele agenta kanálu zpráv) instance kanálu.

Varování: Pověření ve struktuře MQCSP pro klientskou aplikaci jsou někdy odesílána po síti jako prostý text. Chcete-li se ujistit, že jsou pověření aplikace klienta chráněna, prohlédněte si téma “Ochrana heslem MQCSP” na stránce 31.

Použitím řetězce XAOPEN k zadání ID uživatele a hesla se můžete vyhnout změně kódu aplikace.

Poznámka:

V systému IBM WebSphere MQ 6.0umožňuje uživatelská procedura zabezpečení nastavení protokolu MQCSP. Proto klienti na této úrovni nebo novější nemusí být upgradováni.

Ve verzích produktu IBM MQ starších než IBM MQ 8.0však MQCSP nekladlo žádná omezení na ID uživatele a heslo poskytnuté aplikací. Při použití těchto hodnot s funkcemi poskytovanými produktem

IBM MQ existují omezení, která se vztahují na použití těchto funkcí, ale pokud je předáváte pouze svým vlastním východům, tato omezení se nepoužijí.

Související pojmy

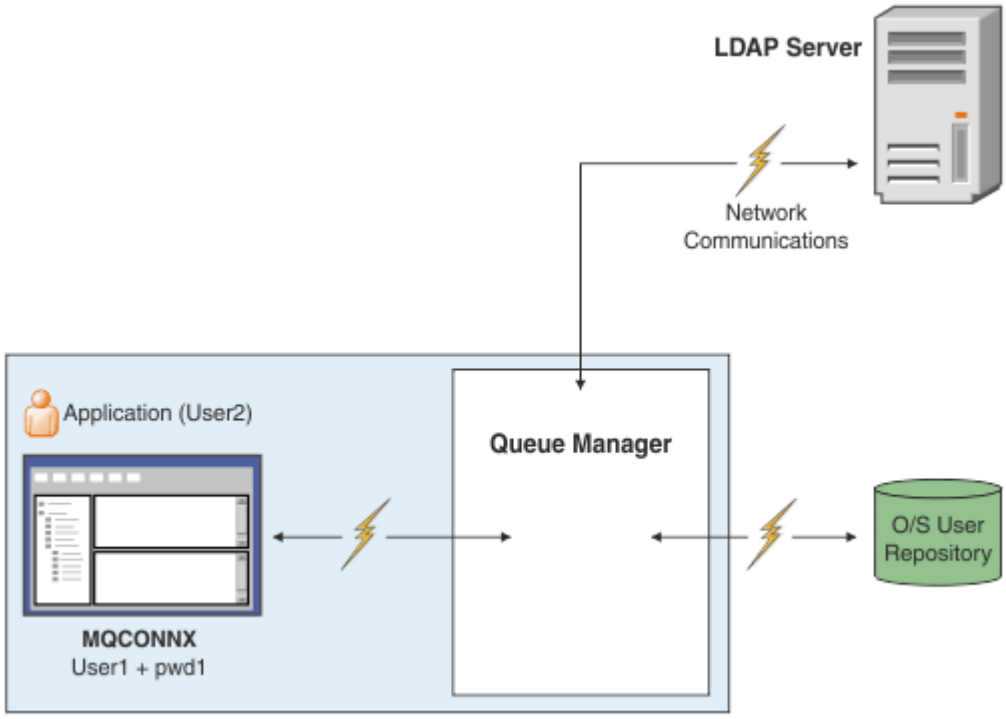
“Ověření připojení” na stránce 70
Ověřování připojení umožňuje aplikacím při připojení ke správci front zadávat ověřovací pověření. Správce front ověřuje pověření. ID uživatele zadané v pověřeních lze také přijmout pro použití při kontrolách autorizace pro prostředky, ke kterým aplikace přistupuje.

“Ověření připojení: Konfigurace” na stránce 71
Správce front lze nakonfigurovat tak, aby ověřoval pověření dodaná aplikací při připojení.

“Ověření připojení: Úložiště uživatelů” na stránce 77
Pro každého z vašich správců front můžete zvolit různé typy objektů ověřovacích informací pro ověřování ID uživatelů a hesel.

Ověření připojení: Úložiště uživatelů

Pro každého z vašich správců front můžete zvolit různé typy objektů ověřovacích informací pro ověřování ID uživatelů a hesel.



Obrázek 7. Typy objektů ověřovacích informací

```
DEFINE AUTHINFO(USE.OS) AUTHTYPE(IDPWOS)
DEFINE AUTHINFO(USE.LDAP) +
AUTHTYPE(IDPWLDAP) +
CONNAME('ldap1(389),ldap2(389)') +
LDAPUSER('CN=QMGR1') +
LDAPPWD('passw0rd') SECCOMM(YES)
```

Existují dva typy objektů ověřovacích informací, jak jsou znázorněny v diagramu:

- `IDPWOS` se používá k označení, že správce front používá lokální operační systém k ověření ID uživatele a hesla. Pokud se rozhodnete použít lokální operační systém, musíte nastavit společné atributy, jak je popsáno v předchozích tématech.
- `IDPWLDAP` se používá k označení, že správce front používá server LDAP k ověření ID uživatele a hesla. Pokud se rozhodnete použít server LDAP, další informace naleznete v tomto tématu.

Pro každého správce front, který má být použit, lze vybrat pouze jeden typ objektu ověřovacích informací, a to pojmenováním příslušného objektu v atributu **CONNAUTH** správce front.

Použití serveru LDAP pro ověření.

Nastavte pole **CONNAME** na adresu serveru LDAP pro správce front. Můžete poskytnout více adres pro server LDAP v seznamu odděleném čárkami, což může pomoci s redundancí, pokud server LDAP neposkytuje toto zařízení sám.

Nastavte požadované ID a heslo serveru LDAP v polích **LDAPUSER** a **LDAPPWD** tak, aby správce front mohl přistupovat k serveru LDAP a vyhledávat informace o záznamech uživatelů.

Zabezpečené připojení k serveru LDAP

Na rozdíl od kanálů neexistuje žádný parametr **SSLCIPH** pro zapnutí použití TLS pro komunikaci se serverem LDAP. V tomto případě produkt IBM MQ vystupuje jako klient pro server LDAP, takže velká část konfigurace se provádí na serveru LDAP. Některé existující parametry v souboru IBM MQ se používají ke konfiguraci toho, jak toto připojení funguje.

Nastavte pole **SECCOMM** , abyste řídili, zda připojitelnost k serveru LDAP používá TLS.

Kromě tohoto atributu atributy správce front **SSLFIPS** a **SUITEB** omezují vybranou sadu specifikací šifer. Certifikát, který se používá k identifikaci správce front na serveru LDAP, je certifikát správce front, buď `ibmwebspheremq` *`qmgr-name`* , nebo hodnota atributu **CERTLABL** . Podrobnosti viz Popisky digitálních certifikátů .

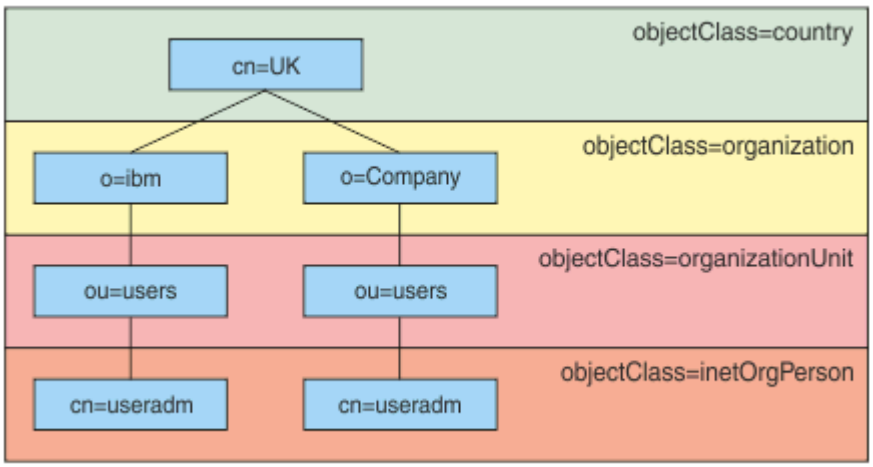
Úložiště uživatelů LDAP

Při použití úložiště uživatelů LDAP je třeba ve správci front provést další konfiguraci, než jen sdělit správci front, kde má být server LDAP nalezen.

ID uživatelů definovaná na serveru LDAP mají hierarchickou strukturu, která je jedinečně identifikuje. Aplikace se proto může připojit ke správci front a prezentovat své ID uživatele jako plně kvalifikované hierarchické ID uživatele.

Chcete-li však zjednodušit informace, které musí aplikace poskytnout, je možné nakonfigurovat správce front tak, aby předpokládal, že první část hierarchie je společná pro všechna ID, a automaticky ji přidat před zkrácené ID poskytnuté aplikací. Správce front pak může serveru LDAP předložit úplné ID.

Nastavte BASEDNU na počáteční bod, ve kterém hledání LDAP hledá ID v hierarchii LDAP. Když nastavíte BASEDNU, musíte se ujistit, že se při hledání ID v hierarchii LDAP vrátí pouze jeden výsledek.



Obrázek 8. Příklad hierarchie LDAP

Například v produktu Obrázek 8 na stránce 78 BASEDNU lze nastavit hodnotu "ou=users, o=ibm, c = UK" nebo ", o=ibm, c = UK". Protože však rozlišující název, který obsahuje "cn = useradm", existuje jak ve větvi "o = ibm", tak ve větvi "o=Company", nemůže být BASEDNU nastaven na "c = UK". Z důvodů výkonu a zabezpečení použijte nejvyšší bod v hierarchii LDAP, ze kterého můžete odkazovat na všechna potřebná ID uživatelů. V tomto příkladu je to "ou=users, o=ibm, c = UK".

Vaše aplikace může odeslat správci front ID uživatele bez zadání názvu atributu LDAP, například `CN=` . Pokud nastavíte USRFIELD na název atributu LDAP, tato hodnota se přidá jako předpona k ID uživatele, které pochází z aplikace. Může se jednat o užitečný migrační prostředek při přechodu z ID uživatelů operačního systému na ID uživatelů LDAP, protože aplikace pak může v obou případech prezentovat stejný řetězec a vyhnout se změně aplikace.

Proto celé ID uživatele prezentované serveru LDAP vypadá takto:

```
USRFIELD = ID_from_application BASEDNU
```

Související pojmy

“Ověření připojení” na stránce 70
Ověřování připojení umožňuje aplikacím při připojení ke správci front zadávat ověřovací pověření. Správce front ověřuje pověření. ID uživatele zadané v pověřeních lze také přijmout pro použití při kontrolách autorizace pro prostředky, ke kterým aplikace přistupuje.

“Ověření připojení: Konfigurace” na stránce 71
Správce front lze nakonfigurovat tak, aby ověřoval pověření dodaná aplikací při připojení.

“Ověření připojení: Změny aplikace” na stránce 76

Uživatelská procedura zabezpečení na straně klienta pro vložení ID uživatele a hesla (`mqccred`)

Máte-li aplikace klienta, které jsou nezbytné pro odeslání ID uživatele nebo hesla, ale ještě nemůžete změnit zdroj, existuje uživatelská procedura pro zabezpečení zprávy dodávaná s názvem IBM MQ 8.0 s názvem **`mqccred`** , kterou můžete použít. Produkt **`mqccred`** poskytuje ID uživatele a heslo pro klientskou aplikaci ze souboru `.ini` . Toto ID uživatele a heslo jsou odeslány správci front, který je bude ověřovat, pokud je k tomu nakonfigurován.

Přehled

`mqccred` je uživatelská procedura pro zabezpečení zprávy, která je spuštěna na stejném počítači jako klientská aplikace. Umožňuje, aby informace o ID uživatele a hesle byly poskytnuty jménem klientské aplikace, pokud tyto informace nejsou poskytovány samotnou aplikací. Informace o ID uživatele a hesle jsou dodávány ve struktuře známé jako Parametry zabezpečení připojení (MQCSP) a budou ověřeny správcem front, pokud je nakonfigurováno ověření připojení .

Informace o ID uživatele a hesle jsou načteny ze souboru `.ini` na klientském počítači. Hesla v souboru jsou chráněna zatemněním pomocí příkazu **`runmqccred`** a také zajištěním, že oprávnění k souboru `.ini` jsou nastavena tak, aby je bylo možné číst pouze ID uživatele, který spouští aplikaci klienta (a tedy i uživatelskou proceduru).

Umístění

Produkt **`mqccred`** je nainstalován:

Windows platformy
V adresáři *`installation_directory`*`\Tools\c\Samples\mqccred\`

AIX and Linux platformy
V adresáři *`installation_directory`*`/samp/mqccred`

Notes: Ukončení:

1. Funguje čistě jako uživatelská procedura kanálu zabezpečení a musí být jedinou takovou uživatelskou procedurou definovanou na kanálu.

2. Obvykle je pojmenován prostřednictvím tabulky CCDT (Client Channel Definition Table), ale klient systému Java může mít uživatelskou proceduru přímo zmíněnou v objektech JNDI, nebo může být uživatelská procedura konfigurována pro aplikace, které ručně konstruují strukturu MQCD .
3. Musíte zkopírovat programy **mqccred** a **mqccred_r** do adresáře `var/mqm/exits` .

   Například na 64bitovém systému AIX nebo Linux zadejte příkaz:

   ```
   cp installation_directory/samp/mqccred/lib64/* /var/mqm/exits
   ```

   Další informace viz Příklad testu mqccred krok za krokem.
4. Lze spustit v předchozích verzích produktu IBM MQ, a to až do verze IBM WebSphere MQ 7.0.1.

Nastavení ID uživatelů a hesel

Soubor `.ini` obsahuje sekce pro každého správce front s globálním nastavením pro neurčené správce front. Každá sekce obsahuje název správce front, ID uživatele a buď prostý text, nebo zamlžené heslo.

Soubor `.ini` musíte upravit ručně pomocí libovolného editoru a přidat atribut hesla ve formátu prostého textu do sekcí. Spusťte poskytnutý program **runmqccred** , který vezme soubor `.ini` a nahradí atribut **Password** atributem **OPW** , zamlžené formě hesla.

Popis příkazu a jeho parametrů viz runmqccred .

Soubor `mqccred.ini` obsahuje informace o ID uživatele a hesle.

Soubor šablony `.ini` je poskytován ve stejném adresáři jako uživatelská procedura, aby poskytoval počáteční bod pro váš podnik.

Standardně bude tento soubor vyhledán v adresáři `$HOME/.mqs/mqccred.ini`. Chcete-li jej vyhledat jinde, můžete použít proměnnou prostředí *MQCCRED* , aby na ni ukazovala:

```
MQCCRED=C:\mydir\mqccred.ini
```

Používáte-li produkt *MQCCRED*, musí proměnná obsahovat úplný název konfiguračního souboru včetně všech typů souborů `.ini` . Vzhledem k tomu, že tento soubor obsahuje hesla (i když jsou zamlžené), očekává se, že budete chránit soubor pomocí oprávnění operačního systému, abyste zajistili, že jej neautorizovaní uživatelé nebudou moci číst. Pokud nemáte správné oprávnění k souboru, uživatelská procedura nebude úspěšně spuštěna.

Pokud aplikace již dodala strukturu MQCSP , uživatelská procedura to obvykle respektuje a nebude vkládat žádné informace ze souboru `.ini` . Můžete ji však přepsat pomocí atributu **Force** v sekci.

Nastavení **Force** na hodnotu *TRUE* odebere ID uživatele a heslo dodané aplikací a nahradí je verzí souboru ini.

Můžete také nastavit atribut **Force** v globální sekci souboru, abyste nastavili výchozí hodnotu tohoto souboru.

Výchozí hodnota parametru **Force** je *FALSE*.

Můžete zadat ID uživatele a heslo pro všechny správce front nebo pro každého jednotlivého správce front. Toto je příklad souboru `mqccred.ini` :

```
# comments are permitted
AllQueueManagers:
User=abc
OPW=%^&aervrgtsr

QueueManager:
Name=QMA
User=user1
OPW=H&^dbgfh

Force=TRUE

QueueManager:
```

```
Name=QMB
User=user2
password=passw0rd
```

Notes:

1. Definice jednotlivých správců front mají přednost před globálním nastavením.
2. Atributy nerozlišují velikost písmen.

Omezení

Když je tato uživatelská procedura používána, lokální ID uživatele osoby, která spouští aplikaci, neproudí z klienta na server. Jediné dostupné informace o identitě jsou z obsahu souboru ini.

Proto musíte nakonfigurovat správce front tak, aby buď používal **ADOPTCTX(YES)**, nebo namapovat příchozí požadavek na připojení na příslušné ID uživatele prostřednictvím jednoho z dostupných mechanizmů, například “Záznamy ověření kanálu” na stránce 51.

Důležité: Pokud přidáte nová hesla nebo aktualizujete stará hesla, příkaz **runmqccred** zpracuje pouze všechna hesla v prostém textu a vaše zamlžené hesla ponechá beze změny.

Ladění

Uživatelská procedura zapisuje do standardního trasování IBM MQ , je-li povoleno.

Pro pomoc při ladění problémů s konfigurací může uživatelská procedura také zapisovat přímo do stdout.

Žádná data uživatelské procedury zabezpečení kanálu (**SCYDATA**) Pro kanál je obvykle vyžadována konfigurace. Můžete však zadat:

ERROR
Vytiskněte pouze informace o chybových stavech, například o tom, že nelze najít konfigurační soubor.

LADĚNÍ
Zobrazí tyto chybové stavy a některé další trasovací příkazy.

NOCHECKS
Vynechá omezení oprávnění k souboru a další omezení, že by soubor `.ini` neměl obsahovat žádná nechráněná hesla.

Do pole **SCYDATA** můžete vložit jeden nebo více těchto prvků oddělených čárkami v libovolném pořadí. Například `SCYDATA=(NOCHECKS,DEBUG)`.

Všimněte si, že položky rozlišují velká a malá písmena a musí být zadány velkými písmeny.

Použití produktu `mqccred`

Jakmile máte nastaven soubor, můžete vyvolat uživatelskou proceduru kanálu tak, že aktualizujete definici kanálu připojení klienta tak, aby obsahovala atribut `SCYEXIT('mqccred(ChlExit)')`:

```
DEFINE CHANNEL(channelname) CHLTYPE(clntconn) +
CONNAME(remote machine) +
QMNAME(remote qmgr) +
SCYEXIT('mqccred(ChlExit)') +
REPLACE
```

Související odkazy

SCYDATA

SCYEXIT

runmqccred

Ověření připojení s klientem Java

Ověřování připojení je funkce v produktu IBM MQ , která umožňuje konfigurovat správce front tak, aby správce front mohl ověřovat aplikace pomocí zadaného jména uživatele a hesla. Pokud se jedná o aplikaci

Java , která používá přenos klienta, lze ověření připojení spustit v režimu kompatibility nebo v režimu ověření MQCSP.

ID uživatele a heslo, které má být ověřeno, je určeno aplikací pomocí jedné z následujících metod:

- V aplikaci IBM MQ classes for Java ve třídě `MQEnvironment` nebo ve vlastnostech hašovací tabulky, které se předávají konstruktoru `com.ibm.mq.MQQueueManager` .
- V aplikaci IBM MQ classes for JMS jako argumenty metody `createConnection(String username, String Password)` nebo `createContext(String username, String password)` .

Režim ověřování MQCSP

V tomto režimu je ID uživatele na straně klienta, pod kterým je aplikace spuštěna, odesláno správci front a také ID uživatele a heslo, které má být ověřeno. IBM MQ classes for Java a IBM MQ classes for JMS odesílají ID uživatele a heslo, které mají být ověřeny, do správce front ve struktuře MQCSP .

ID uživatele a heslo jsou k dispozici pro uživatelskou proceduru zabezpečení připojení serveru v rámci struktury MQCSP. Adresu struktury MQCSP lze najít v poli **SecurityParms** struktury MQCXP pro daný kanál.

Režim ověřování MQCSP má následující výhody:

- Maximální délka ID uživatele, které má být ověřeno, je 1024 znaků.
- Maximální délka hesla pro ověření je 256 znaků.
- Kontroly autorizace pro přístup k použití prostředků produktu IBM MQ lze provést pomocí ID uživatele na straně klienta, pod kterým je aplikace spuštěna, když je objekt ověřovacích informací, který se používá k řízení ověření připojení ve správci front, nakonfigurován s pomocí metody ADOPTCTX (NO).

Režim kompatibility

Před produktem IBM MQ 8.0mohl klient produktu Java odeslat ID uživatele a heslo v rámci kanálu připojení klienta kanálu připojení serveru a předat je uživatelské proceduře zabezpečení v polích **RemoteUserIdentifier** a **RemotePassword** struktury MQCD. V režimu kompatibility je toto chování zachováno.

Tento režim můžete použít v kombinaci s ověřením připojení a migrovat mimo všechny uživatelské procedury zabezpečení, které byly dříve použity k provedení stejné úlohy.

Tento režim má následující omezení:

- Délka ID uživatele a hesla musí být 12 znaků nebo méně. ID uživatelů delší než 12 znaků jsou zkrácena na 12 znaků. To může způsobit selhání připojení s kódem příčiny MQRC_NOT_AUTHORIZED.
- ID uživatele na straně klienta, pod kterým je aplikace spuštěna, není odesláno správci front. Musíte buď nastavit volbu ADOPTCTX (YES) na objektu ověřovacích informací, který se používá k řízení ověření připojení ve správci front, nebo použít jinou metodu, například pravidlo ověřování kanálu založené na certifikátu TLS, abyste nastavili ID uživatele kanálu MCA, u kterého se kontroluje autorizace pro použití prostředků IBM MQ .

Výchozí režim ověření

Výchozí režim ověřování používaný klientskou aplikací IBM MQ classes for Java nebo IBM MQ classes for JMS se liší v závislosti na tom, zda aplikace určuje ID uživatele a heslo.

- V 9.3.0 Pokud je v produktu IBM MQ 9.2.1zadáno ID uživatele a heslo, použije se standardně ověření MQCSP.
- Je-li ve verzích starších než IBM MQ 9.2.1uvedeno ID uživatele a heslo, výchozí režim je následující:
  - Ověřování MQCSP je standardně používáno aplikacemi, které používají protokol IBM MQ classes for Java.
  - Režim kompatibility je standardně používán aplikacemi, které používají IBM MQ classes for JMS.

- Pokud je zadáno ID uživatele, ale není zadáno žádné heslo, použije se standardně režim kompatibility.
- Není-li uvedeno žádné ID uživatele, použije se vždy režim kompatibility.

V případech, kdy je zadáno ID uživatele, může aplikace zvolit specifický režim ověření pro každé individuální připojení, nebo jej nastavit globálně před spuštěním aplikace, jak je popsáno v tématu "Výběr režimu ověření" na stránce 83.

Poznámka: V 9.3.0 Aplikace, které používají produkt IBM MQ classes for JMS , mohou být ovlivněny změnou výchozího režimu ověření v produktu IBM MQ 9.3.0. Po upgradu produktu IBM MQ classes for JMS na verzi IBM MQ 9.3.0budou aplikace, které dříve standardně používaly režim kompatibility, místo toho používat ověřování MQCSP. To může způsobit, že se aplikace, které se dříve úspěšně připojily ke správci front, nedokáží připojit s kódem příčiny `JMSException` obsahujícím kód příčiny 2035 (MQRC_NOT_AUTHORIZED). Pokud k tomu dojde, použijte jednu z metod popsaných v části "Výběr režimu ověření" na stránce 83 k určení, že aplikace používá režim kompatibility.

Aplikace systému Java , které se připojují ke správci front pomocí lokálních vazeb, vždy používají režim ověřování MQCSP.

Výběr režimu ověření

Režim ověřování používaný aplikacemi klienta Java , které určují jméno uživatele při připojování ke správci front, lze určit pomocí jedné z následujících metod. Tyto metody jsou uvedeny v sestupném pořadí podle priority. Není-li režim ověřování určen pomocí žádné z těchto metod, použije se výchozí režim ověřování.

Poznámka: V 9.3.0 Použití těchto metod k výběru režimu ověření bylo vyjasněno v souboru IBM MQ 9.3.0. V některých případech se může režim ověřování používaný klientskou aplikací Java změnit, když je produkt IBM MQ classes for Java nebo IBM MQ classes for JMS upgradován na IBM MQ 9.3.0. To může způsobit, že se aplikace, které se dříve úspěšně připojily ke správci front, nedokáží připojit s kódem příčiny `JMSException` obsahujícím kód příčiny 2035 (MQRC_NOT_AUTHORIZED). Pokud k tomu dojde, vyberte požadovaný režim ověření pomocí jedné z následujících metod.

- Určete režim ověřování pro jednotlivá připojení nastavením příslušné vlastnosti v aplikaci před připojením ke správci front.
  - Při použití parametru IBM MQ classes for Javanastavte vlastnost *MQConstants.USE_MQCSP_AUTHENTICATION_PROPERTY* ve vlastnostech hašovací tabulky, která je předána konstruktoru `com.ibm.mq.MQQueueManager` .
  - Při použití IBM MQ classes for JMSnastavte vlastnost *JmsConstants.USER_AUTHENTICATION_MQCSP* v příslušné továrně připojení před vytvořením připojení.

  Nastavte hodnotu těchto vlastností na jednu z následujících hodnot:

  ano
  Při ověřování se správcem front používejte režim ověřování MQCSP.

  ne
  Při ověřování se správcem front použijte režim kompatibility.
- Určete režim ověřování pro všechna připojení klienta provedená aplikací nastavením systémové vlastnosti *com.ibm.mq.cfg.jmqi.useMQCSPauthentication* Java při spouštění aplikace. Nastavte hodnotu vlastnosti na jednu z následujících hodnot:

  Y
  Při ověřování se správcem front používejte režim ověřování MQCSP.

  N
  Při ověřování se správcem front použijte režim kompatibility.

  Následující příkaz například nastaví vlastnost na výběr režimu kompatibility a spustí aplikaci Java :

  ```
  java -Dcom.ibm.mq.cfg.jmqi.useMQCSPauthentication=N application_name
  ```
- Nastavením proměnné prostředí *com.ibm.mq.jmqi.useMQCSPauthentication* v prostředí, ve kterém je aplikace spuštěna, určete režim ověřování pro všechna připojení klienta, která byla vytvořena

aplikacemi spuštěnými ve stejném prostředí. Nastavte hodnotu proměnné prostředí na jednu z následujících hodnot:

Y
Při ověřování se správcem front používejte režim ověřování MQCSP.

N
Při ověřování se správcem front použijte režim kompatibility.

- Určete režim ověřování pro všechny aplikace, které používají specifický konfigurační soubor klienta IBM MQ MQI client , zadáním atributu **useMQCSPauthentication** v sekci JMQI konfiguračního souboru klienta. Nastavte hodnotu atributu na jednu z následujících hodnot:

  YES
  Při ověřování se správcem front používejte režim ověřování MQCSP.

  NO
  Při ověřování se správcem front použijte režim kompatibility.

  Další informace o atributu **useMQCSPauthentication** naleznete v části Sekce JMQI konfiguračního souboru klienta.

Výběr režimu ověření v produktu IBM MQ Explorer

IBM MQ Explorer je aplikace Java , takže tyto dva režimy, režim kompatibility a režim ověření MQCSP, jsou použitelné i pro tuto aplikaci.

V produktu IBM MQ 9.1.0je výchozí režim ověřování MQCSP. Před volbou IBM MQ 9.1je výchozí režim kompatibility.

Na panelech, kde je uvedena identifikace uživatele, je zaškrtávací políčko pro povolení nebo zakázání režimu kompatibility:

- V systému IBM MQ 9.1.0není toto zaškrtávací políčko standardně zaškrtnuto. Chcete-li použít režim kompatibility, zaškrtněte toto políčko.
- Před IBM MQ 9.1.0je standardně toto zaškrtávací políčko povoleno. Chcete-li použít ověření MQCSP, zrušte zaškrtnutí políčka.

Související pojmy
“Ověření připojení” na stránce 70
Ověřování připojení umožňuje aplikacím při připojení ke správci front zadávat ověřovací pověření. Správce front ověřuje pověření. ID uživatele zadané v pověřeních lze také přijmout pro použití při kontrolách autorizace pro prostředky, ke kterým aplikace přistupuje.

“Ověření připojení: Změny aplikace” na stránce 76

“Ověření připojení: Úložiště uživatelů” na stránce 77
Pro každého z vašich správců front můžete zvolit různé typy objektů ověřovacích informací pro ověřování ID uživatelů a hesel.

Zabezpečení zpráv v adresáři IBM MQ

Zabezpečení zpráv v infrastruktuře IBM MQ poskytuje produkt Advanced Message Security.

Advanced Message Security (AMS) rozšiřuje služby zabezpečení produktu IBM MQ tak, aby poskytovaly podepisování a šifrování dat na úrovni zpráv. Rozšířené služby zaručují, že data zpráv nebyla změněna mezi tím, kdy byla původně umístěna do fronty, a tím, kdy byla načtena. Kromě toho produkt AMS ověřuje, zda je odesilatel dat zprávy autorizován k umístění podepsaných zpráv do cílové fronty.

Související pojmy
“Advanced Message Security” na stránce 613
Advanced Message Security (AMS) je komponenta produktu IBM MQ , která poskytuje vysokou úroveň ochrany citlivých dat procházejících sítí IBM MQ , aniž by to mělo vliv na koncové aplikace.

Plánování požadavků na zabezpečení

Tato kolekce témat vysvětluje, co je třeba zvážit při plánování zabezpečení v prostředí IBM MQ .

Produkt IBM MQ můžete použít pro širokou škálu aplikací na různých platformách. Požadavky na zabezpečení se pravděpodobně budou pro každou aplikaci lišit. Pro některé z nich bude bezpečnost kritickým aspektem.

Produkt IBM MQ poskytuje řadu služeb zabezpečení na úrovni odkazů, včetně podpory protokolu TLS (Transport Layer Security).

Při plánování instalace produktu IBM MQmusíte zvážit některé aspekty zabezpečení:

- Multi Pokud v systému Multiplatformstyto aspekty ignorujete a neděláte nic, nemůžete použít IBM MQ.
- z/OS V systému z/OSje ignorování těchto aspektů důsledkem toho, že vaše prostředky IBM MQ jsou nechráněné. To znamená, že všichni uživatelé mohou přistupovat ke všem prostředkům IBM MQ a měnit je.

Oprávnění ke správě IBM MQ

Administrátoři produktu IBM MQ potřebují oprávnění k:

- Zadejte příkazy pro administraci produktu IBM MQ
- PoužijteIBM MQ Explorer
- IBM i Použijte administrativní panely a příkazy IBM i .
- z/OS Použijte operace a ovládací panely na z/OS
- z/OS Použijte obslužný program IBM MQ , CSQUTIL, na systému z/OS
- z/OS Přístup k datovým sadám správce front v systému z/OS

Další informace naleznete v následujících tématech:

- ALW “Oprávnění ke správě IBM MQ v systému AIX, Linux, and Windows” na stránce 419
- IBM i “Oprávnění ke správě IBM MQ v systému IBM i” na stránce 90
- z/OS “Oprávnění ke správě IBM MQ v systému z/OS” na stránce 90

Oprávnění k práci s objekty IBM MQ

Aplikace mohou přistupovat k následujícím objektům produktu IBM MQ pomocí volání MQI:

- Správci front
- Fronty
- Procesy
- Seznamy názvů
- Témata

Aplikace mohou také používat příkazy PCF (Programmable Command Format) pro přístup k těmto objektům IBM MQ a pro přístup ke kanálům a objektům ověřovacích informací. Tyto objekty mohou být chráněny produktem IBM MQ tak, aby ID uživatelů přidružená k aplikacím potřebovala oprávnění pro přístup k nim.

Další informace viz “Autorizace pro použití aplikací IBM MQ” na stránce 92.

Zabezpečení kanálu

ID uživatelů přidružená k agentům kanálu zpráv (MCA) potřebují oprávnění pro přístup k různým prostředkům IBM MQ . Například agent MCA musí být schopen se připojit ke správci front. Pokud se jedná o odesílající MCA, musí být schopen otevřít přenosovou frontu pro kanál. Jedná-li se o přijímající agenta MCA, musí být schopen otevřít cílové fronty. ID uživatelů přidružená k aplikacím, které potřebují spravovat kanály, iniciátory kanálů a moduly listener, potřebují oprávnění k použití příslušných příkazů PCF. Většina aplikací však takový přístup nepotřebuje.

Další informace viz “Autorizace kanálu” na stránce 113.

Další aspekty

Následující aspekty zabezpečení je třeba zvážit pouze v případě, že používáte určité funkce IBM MQ nebo rozšíření základního produktu:

- “Zabezpečení pro klastry správců front” na stránce 126
- “Zabezpečení pro publikování/odběr IBM MQ” na stránce 126
- “Zabezpečení pro IBM MQ Internet Pass-Thru” na stránce 128

Identifikace a ověření plánování

Rozhodněte, která ID uživatelů použít a jak a na jakých úrovních chcete použít ovládací prvky ověření.

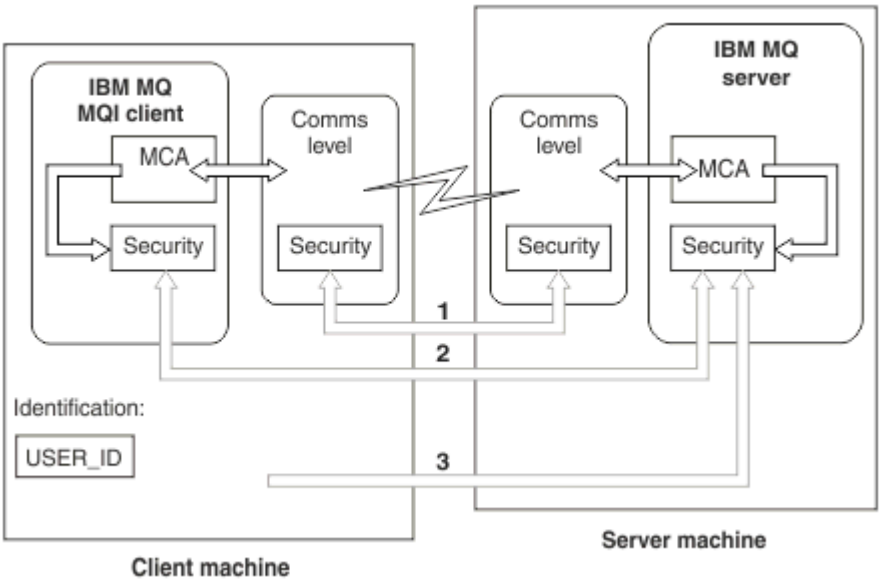
Musíte se rozhodnout, jak budete identifikovat uživatele svých aplikací IBM MQ , s ohledem na to, že různé operační systémy podporují ID uživatelů různých délek. Záznamy ověřování kanálu můžete použít k mapování z jednoho ID uživatele na jiné nebo k určení ID uživatele na základě některého atributu připojení. Kanály IBM MQ používající TLS používají digitální certifikáty jako mechanizmus pro identifikaci a ověření. Každý digitální certifikát má rozlišující název subjektu, který lze mapovat na specifické identity pomocí záznamů ověřování kanálu. Kromě toho certifikáty CA v úložišti klíčů určují, které digitální certifikáty lze použít k ověření v produktu IBM MQ. Další informace viz:

- “Mapování vzdáleného správce front na ID uživatele MCAUSER” na stránce 405
- “Mapování ID uživatele klienta na ID uživatele MCAUSER” na stránce 406
- “Mapování rozlišujícího názvu SSL nebo TLS na ID uživatele MCAUSER” na stránce 407
- “Mapování adresy IP na ID uživatele MCAUSER” na stránce 409

Plánování ověření pro aplikaci klienta

Ovládací prvky ověření můžete použít na čtyřech úrovních: na úrovni komunikace, v uživatelských procedurách zabezpečení, se záznamy ověření kanálu a ve smyslu identifikace, která je předána uživatelské proceduře zabezpečení.

Existují čtyři úrovně zabezpečení, které je třeba zvážit. Diagram zobrazuje IBM MQ MQI client , který je připojen k serveru. Zabezpečení se používá na čtyřech úrovních, jak je popsáno v následujícím textu. MCA je agent kanálu zpráv.



Obrázek 9. Zabezpečení v připojení klient/server

1. Úroveň komunikace

   Viz šipka 1. Chcete-li implementovat zabezpečení na úrovni komunikace, použijte protokol TLS. Další informace viz “Šifrovací bezpečnostní protokoly: TLS” na stránce 18

2. Záznamy ověření kanálu

   Viz šipky 2 & 3. Ověřování lze řídit pomocí rozlišujících názvů adresy IP nebo protokolu TLS na úrovni zabezpečení. ID uživatele může být také blokováno nebo deklarovaný ID uživatele může být namapován na platné ID uživatele. Úplný popis je uveden v souboru “Záznamy ověření kanálu” na stránce 51.

3. Ověření připojení

   Viz šipka 3. Klient odešle ID uživatele a heslonebo token ověření. Další informace viz téma “Ověření připojení: Konfigurace” na stránce 71.

4. Uživatelské procedury zabezpečení kanálu

   Viz šipka 2. Uživatelské procedury zabezpečení kanálu pro komunikaci mezi klientem a serverem mohou pracovat stejným způsobem jako pro komunikaci mezi servery. Dvojice uživatelských procedur nezávislých na protokolu může být napsána tak, aby poskytovala vzájemné ověření klienta i serveru. Úplný popis je uveden v části Programy uživatelských procedur pro zabezpečení zprávy kanálu.

5. Identifikace předaná uživatelské proceduře zabezpečení kanálu

   Viz šipka 3. V komunikaci mezi klientem a serverem nemusí uživatelské procedury zabezpečení kanálu fungovat jako dvojice. Uživatelská procedura na straně klienta IBM MQ může být vynechána. V tomto případě je ID uživatele umístěno do deskriptoru kanálu (MQCD) a uživatelská procedura zabezpečení na straně serveru jej může v případě potřeby změnit.

   Produkt IBM MQ MQI clients také odešle další informace, které vám pomohou s identifikací.

   - ID uživatele, které je předáno na server, je momentálně přihlášené ID uživatele na klientovi.
   - ID zabezpečení momentálně přihlášeného uživatele.

   Hodnoty ID uživatele, a je-li k dispozici, ID zabezpečení, mohou být použity uživatelskou procedurou pro zabezpečení serveru k zavedení identity produktu IBM MQ MQI client.

Z produktu IBM MQ 8.0můžete odesílat hesla, která jsou zahrnuta ve struktuře MQCSP.

Linux V 9.3.4 AIX From IBM MQ 9.3.4, IBM MQ MQI clients connecting to IBM MQ queue managers running on AIX or Linux systems can also send authentication tokens in the MQCSP structure.

Varování: V některých případech je heslo nebo token ověření ve struktuře MQCSP pro klientskou aplikaci odesláno v síti jako prostý text. Chcete-li se ujistit, že jsou hesla aplikace klienta a tokeny ověření odpovídajícím způsobem chráněny, prohlédněte si téma “Ochrana heslem MQCSP” na stránce 31.

ID uživatelů

Při vytváření ID uživatelů pro klientské aplikace nesmí být ID uživatelů delší než maximální povolená délka. Nesmíte používat vyhrazená ID uživatelů UNKNOWN a NOBODY. Pokud je server, ke kterému se klient připojuje, serverem IBM MQ for Windows , musíte se vyhnout použití znaku zavináč, @. Povolená délka ID uživatelů závisí na platformě, která se používá pro server:

- z/OS Linux AIX V systému z/OS, AIX and Linuxje maximální délka ID uživatele 12 znaků.
- IBM i V systému IBM ije maximální délka ID uživatele 10 znaků.
- Windows V systému Windowsplatí, že pokud jsou server IBM MQ MQI client i server IBM MQ na systému Windowsa server má přístup k doméně, ve které je definováno ID uživatele klienta, maximální délka ID uživatele je 20 znaků. Pokud však server IBM MQ není serverem Windows , je ID uživatele zkráceno na 12 znaků.
- Používáte-li strukturu MQCSP k předávání pověření, maximální délka ID uživatele je 1024 znaků. ID uživatele struktury MQCSP nelze použít k obcházení maximální délky ID uživatele použité produktem IBM MQ pro autorizaci. Další informace o struktuře MQCSP viz “Identifikace a ověřování uživatelů pomocí struktury MQCSP” na stránce 345.

Na systémech AIX and Linux je předvolba, že se ID uživatelů používají k ověření a skupiny se používají k autorizaci. Tyto systémy však můžete nakonfigurovat tak, aby se autorizovaly vůči ID uživatelů. Další informace viz téma “Oprávnění založená na uživateli OAM na AIX and Linux” na stránce 373. Systémy Windows mohou používat ID uživatelů jak pro ověření, tak pro autorizaci a skupiny pro autorizaci.

Pokud vytvoříte servisní účty, aniž byste věnovali pozornost skupinám, a autorizujete všechna ID uživatelů jinak, může každý uživatel přistupovat k informacím každého jiného uživatele.

Omezená ID uživatelů

ID uživatelů `UNKNOWN` a skupina `NOBODY` mají speciální význam pro IBM MQ. Vytvoření ID uživatele v operačním systému s názvem `UNKNOWN` nebo ve skupině s názvem `NOBODY` může mít nechtěné výsledky.

ID uživatelů při připojování k serveru IBM MQ for Windows

Windows

Server IBM MQ for Windows nepodporuje připojení k serveru IBM MQ MQI client , pokud je klient spuštěn pod ID uživatele, které obsahuje znak @, například `abc@d`. Návratový kód volání `MQCONN` v klientu je MQRC_NOT_AUTHORIZED.

ID uživatele však můžete zadat pomocí dvou znaků @, například `abc@@d`. Použití formátu `id@domain` je upřednostňovaným postupem, abyste se ujistili, že je ID uživatele interpretováno konzistentně ve správné doméně; tedy `abc@@d@domain`.

Autorizace plánování

Naplánujte uživatele, kteří budou mít administrativní oprávnění, a naplánujte, jak autorizovat uživatele aplikací, aby vhodně používali objekty IBM MQ , včetně těch, kteří se připojují z produktu IBM MQ MQI client.

Jednotlivcům nebo aplikacím musí být udělen přístup, aby mohli používat produkt IBM MQ. To, jaký přístup vyžadují, závisí na rolích, které vykonávají, a na úlohách, které musí vykonávat. Autorizaci v produktu IBM MQ lze rozdělit do dvou hlavních kategorií:

- Oprávnění k provádění administrativních operací
- Autorizace pro použití aplikací IBM MQ

Obě provozní třídy jsou řízeny stejnou komponentou a jednotlivci lze udělit oprávnění k provedení obou kategorií operací.

Následující témata poskytují další informace o specifických oblastech autorizace, které musíte zvážit:

Oprávnění ke správě IBM MQ

Administrátoři produktu IBM MQ potřebují oprávnění k provádění různých funkcí. Tento orgán je získán různými způsoby na různých platformách.

Administrátoři produktu IBM MQ potřebují oprávnění k:

- Zadejte příkazy pro správu produktu IBM MQ.
- Windows Linux Použijte IBM MQ Explorer.
- z/OS Použijte operace a ovládací panely na systému z/OS.
- z/OS Použijte obslužný program IBM MQ , CSQUTIL, na systému z/OS.
- z/OS Přistupte k datovým sadám správce front v systému z/OS.

Další informace naleznete v tématu týkajícím se operačního systému.

ALW *Oprávnění ke správě IBM MQ na systémech AIX, Linux, and Windows*

Administrátor systému IBM MQ je členem skupiny mqm. Tato skupina má přístup ke všem prostředkům systému IBM MQ a může vydávat řídicí příkazy systému IBM MQ . Administrátor může udělit specifická oprávnění ostatním uživatelům.

Chcete-li být IBM MQ administrátorem systémů AIX, Linux, and Windows , musí být uživatel členem skupiny *mqm*. Tato skupina se vytvoří automaticky při instalaci produktu IBM MQ. Chcete-li uživatelům povolit zadávání řídicích příkazů, musíte je přidat do skupiny mqm. To zahrnuje uživatele root v systému AIX and Linux.

Uživatelům, kteří nejsou členy skupiny mqm, mohou být udělena oprávnění k administraci, ale nemohou vydávat řídicí příkazy IBM MQ a mají oprávnění spouštět pouze příkazy, pro které jim byl udělen přístup.

Na systémech Windows mají navíc účty SYSTEM a Administrator úplný přístup k prostředkům IBM MQ .

Všichni členové skupiny mqm mají přístup ke všem prostředkům IBM MQ v systému, včetně možnosti spravovat libovolného správce front spuštěného v systému. Tento přístup lze odvolat pouze odebráním uživatele ze skupiny mqm. V systémech Windows mají členové skupiny administrátorů také přístup ke všem prostředkům IBM MQ .

Administrátoři mohou použít řídicí příkaz **runmqsc** k zadání příkazů skriptu IBM MQ Script (MQSC). Je-li příkaz **runmqsc** použit v nepřímém režimu k odeslání příkazů MQSC vzdálenému správci front, je každý příkaz MQSC zapouzdřen v rámci příkazu Escape PCF. Administrátoři musí mít nezbytná oprávnění pro zpracování příkazů MQSC vzdáleným správcem front.

Produkt IBM MQ Explorer vydává příkazy PCF k provádění administrativních úloh. Administrátoři nepotřebují žádná další oprávnění k použití produktu IBM MQ Explorer k administraci správce front v lokálním systému. Je-li produkt IBM MQ Explorer používán k administraci správce front v jiném systému, musí mít administrátoři potřebná oprávnění pro příkazy PCF, které má vzdálený správce front zpracovat.

Další informace o kontrolách oprávnění provedených při zpracování příkazů PCF a MQSC naleznete v následujících tématech:

- Informace o příkazech, které pracují se správci front, frontami, kanály, procesy, seznamy názvů a objekty ověřovacích informací naleznete v části “Autorizace pro použití aplikací IBM MQ” na stránce 92.
- Informace o příkazech, které pracují na kanálech, inicializátorech kanálů, modulech listener a klastrech, naleznete v tématu Zabezpečení kanálu.
- z/OS Informace o příkazech MQSC, které jsou zpracovány příkazovým serverem v systému IBM MQ for z/OS, naleznete v části “Zabezpečení příkazů a zabezpečení prostředků příkazů v systému z/OS” na stránce 91.

Další informace o oprávnění, které potřebujete ke správě systémů IBM MQ for AIX, Linux, and Windows , naleznete v souvisejících informacích.

IBM i *Oprávnění ke správě IBM MQ v systému IBM i*

Chcete-li být IBM MQ administrátorem produktu IBM i, musíte být členem *skupiny QMQMADM*. Tato skupina má vlastnosti podobné vlastnostem skupiny mqm na systémech AIX, Linux, and Windows . Skupina QMQMADM je vytvořena zejména při instalaci produktu IBM MQ for IBM ia členové skupiny QMQMADM mají přístup ke všem prostředkům produktu IBM MQ v systému. Máte také přístup ke všem prostředkům IBM MQ , pokud máte oprávnění *ALLOBJ.

Administrátoři mohou k administraci produktu IBM MQpoužívat příkazy CL.Jedním z těchto příkazů je GRTMQMAUT, který se používá k udělení oprávnění ostatním uživatelům. Jiný příkaz STRMQMMQSC umožňuje administrátorovi zadávat příkazy MQSC lokálnímu správci front.

Existují dvě skupiny CL příkazů, které poskytuje IBM MQ for IBM i:

Skupina 1
Chcete-li zadat příkaz v této kategorii, musí být uživatel členem skupiny QMQMADM nebo musí mít oprávnění *ALLOBJ. Například GRTMQMAUT a STRMQMMQSC patří do této kategorie.

Skupina 2
Chcete-li zadat příkaz v této kategorii, uživatel nemusí být členem skupiny QMQMADM nebo mít oprávnění *ALLOBJ. Místo toho jsou vyžadovány dvě úrovně oprávnění:

- Uživatel vyžaduje oprávnění IBM i pro použití příkazu. Toto oprávnění je uděleno pomocí příkazu GRTOBJAUT.
- Uživatel vyžaduje oprávnění IBM MQ pro přístup k libovolnému objektu IBM MQ přidruženému k příkazu. Toto oprávnění je uděleno pomocí příkazu GRTMQMAUT.

Následující příklady ukazují příkazy v této skupině:

- CRTMQMQ, Vytvořit frontu MQM
- CHGMQMPRC, Změna procesu MQM
- DLTMQMNL, Odstranit seznam názvů MQM
- DSPMQMAUTI, Zobrazení ověřovacích informací MQM
- CRTMQMCHL, Vytvořit kanál MQM

Další informace o této skupině příkazů viz “Autorizace pro použití aplikací IBM MQ” na stránce 92.

Úplný seznam příkazů skupiny 1 a skupiny 2 naleznete v tématu “Přístupová oprávnění pro objekty IBM MQ na IBM i” na stránce 159 .

Další informace o oprávnění, které potřebujete spravovat IBM MQ v systému IBM i, naleznete v tématu Administrace IBM i .

z/OS *Oprávnění ke správě IBM MQ v systému z/OS*

Tato kolekce témat popisuje různé aspekty oprávnění, které potřebujete ke správě produktu IBM MQ for z/OS.

z/OS *Kontroly oprávnění na z/OS*

Produkt IBM MQ for z/OS používá prostředek SAF (System Authorization Facility) ke směrování požadavků na kontroly oprávnění do externího správce zabezpečení (ESM), například do zařízení z/OS Security Server Resource Access Control Facility (RACF). IBM MQ neprovádí žádné vlastní kontroly oprávnění.

Předpokládá se, že jako ESM používáte produkt RACF . Pokud používáte jiný ESM, možná budete muset interpretovat informace poskytnuté pro RACF způsobem, který je relevantní pro váš ESM.

Můžete určit, zda chcete zapnout nebo vypnout kontroly oprávnění pro každého správce front jednotlivě nebo pro každého správce front ve skupině sdílení front.Tato úroveň řízení se nazývá *zabezpečení subsystému*. Pokud vypnete zabezpečení subsystému pro konkrétního správce front, nebudou pro tohoto správce front provedeny žádné kontroly oprávnění.

Pokud zapnete zabezpečení subsystému pro konkrétního správce front, lze kontroly oprávnění provádět na dvou úrovních:

Zabezpečení na úrovni skupiny sdílení front
: Kontroly oprávnění používají profily RACF , které jsou sdíleny všemi správci front ve skupině sdílení front. To znamená, že existuje méně profilů, které je třeba definovat a udržovat, což usnadňuje administraci zabezpečení.

zabezpečení na úrovni správce front
: Kontroly oprávnění používají profily RACF specifické pro správce front.

Můžete použít kombinaci skupiny sdílení front a zabezpečení na úrovni správce front. Můžete například uspořádat profily specifické pro správce front tak, aby potlačovaly profily skupiny sdílení front, do které patří.

Zabezpečení subsystému, zabezpečení na úrovni skupiny sdílení front a zabezpečení na úrovni správce front jsou zapnuty nebo vypnuty definováním *profilů přepínače*. Profil přepínače je normální profil RACF , který má speciální význam pro IBM MQ.

z/OS *Zabezpečení příkazů a zabezpečení prostředků příkazů v systému z/OS*

Zabezpečení příkazu se týká oprávnění k vydání příkazu; oprávnění k prostředku příkazu se týká oprávnění k provedení operace na prostředku. Obě jsou implementovány y pomocí tříd RACF .

Kontroly oprávnění se provádějí, když administrátor produktu IBM MQ vydá příkaz MQSC. Tomu se říká *zabezpečení příkazu*.

Chcete-li implementovat zabezpečení příkazů, musíte definovat určité profily RACF a poskytnout nezbytné skupiny a ID uživatelů přístup k těmto profilům na požadovaných úrovních. Název profilu pro zabezpečení příkazu obsahuje název příkazu MQSC.

Některé příkazy MQSC provádějí operaci na prostředku IBM MQ , například příkaz DEFINE QLOCAL pro vytvoření lokální fronty. Když administrátor zadá příkaz MQSC, provedou se kontroly oprávnění, aby se zjistilo, zda lze požadovanou operaci provést na prostředku uvedeném v příkazu. Nazývá se *zabezpečení prostředků příkazu*.

Chcete-li implementovat zabezpečení prostředků příkazu, musíte definovat určité profily RACF a poskytnout potřebným skupinám a ID uživatelů přístup k těmto profilům na požadovaných úrovních. Název profilu pro zabezpečení prostředků příkazu obsahuje název prostředku IBM MQ a jeho typ (QUEUE, PROCESS, NAMELIST, TOPIC, AUTHINFO nebo CHANNEL).

Zabezpečení příkazů a zabezpečení prostředků příkazů jsou nezávislé. Například, když administrátor zadá příkaz:

```
DEFINE QLOCAL(MOON.EUROPA)
```

jsou prováděny tyto kontroly oprávnění:

- Zabezpečení příkazu kontroluje, zda je administrátor oprávněn zadat příkaz DEFINE QLOCAL.
- Zabezpečení prostředků příkazu kontroluje, zda je administrátor autorizován k provedení operace v lokální frontě s názvem MOON.EUROPA.

Zabezpečení příkazů a zabezpečení prostředků příkazů lze zapnout nebo vypnout definováním profilů přepínačů.

z/OS *Příkazy MQSC a vstupní fronta systémových příkazů v systému z/OS*

V tomto tématu jsou uvedeny informace o tom, jak příkazový server zpracovává příkazy MQSC směrované do vstupní fronty systémových příkazů v systému z/OS.

Zabezpečení příkazů a zabezpečení prostředků příkazů se také používají, když příkazový server načte zprávu obsahující příkaz MQSC ze vstupní fronty systémových příkazů.ID uživatele, které se používá pro kontroly oprávnění, je ID uživatele, které se nachází v poli *UserIdentifier* v deskriptoru zprávy obsahující příkaz MQSC. Toto ID uživatele musí mít požadovaná oprávnění pro správce front, kde je příkaz zpracován. Další informace o poli *UserIdentifier* a způsobu jeho nastavení naleznete v tématu Kontext zprávy.

Zprávy obsahující příkazy MQSC jsou odesílány do vstupní fronty systémových příkazů za následujících okolností:

- Operační a řídicí panely odesílají příkazy MQSC do vstupní fronty systémových příkazů cílového správce front. Příkazy MQSC odpovídají akcím, které jste vybrali na panelech. Pole *UserIdentifier* v každé zprávě je nastaveno na ID uživatele TSO administrátora.
- Funkce COMMAND obslužného programu IBM MQ , CSQUTIL, odešle příkazy MQSC ve vstupní datové sadě do vstupní fronty systémových příkazů cílového správce front. Funkce COPY a EMPTY odesílají příkazy DISPLAY QUEUE a DISPLAY STGCLASS. Pole *UserIdentifier* v každé zprávě je nastaveno na ID uživatele úlohy.
- Příkazy MQSC v datových sadách CSQINPX jsou odesílány do vstupní fronty systémových příkazů správce front, ke kterému je inicializátor kanálu připojen. Pole *UserIdentifier* v každé zprávě je nastaveno na ID uživatele adresního prostoru inicializátoru kanálu.

  Při zadávání příkazů MQSC z datových sad CSQINP1 a CSQINP2 se neprovádějí žádné kontroly oprávnění. Pomocí ochrany datových sad RACF můžete řídit, kdo může aktualizovat tyto datové sady.
- V rámci skupiny sdílení front může iniciátor kanálu odeslat příkazy START CHANNEL do vstupní fronty systémových příkazů správce front, ke kterému je připojen. Příkaz je odeslán při spuštění odchozího kanálu, který používá sdílenou přenosovou frontu. Pole *UserIdentifier* v každé zprávě je nastaveno na ID uživatele adresního prostoru inicializátoru kanálu.
- Aplikace může odesílat příkazy MQSC do vstupní fronty systémových příkazů. Standardně je pole *UserIdentifier* v každé zprávě nastaveno na ID uživatele přidružené k aplikaci.
- V systémech AIX, Linux, and Windows lze řídicí příkaz **runmqsc** použít v nepřímém režimu k odeslání příkazů MQSC do vstupní fronty systémových příkazů správce front v systému z/OS. Pole *UserIdentifier* v každé zprávě je nastaveno na ID uživatele administrátora, který zadal příkaz **runmqsc** .

z/OS *Přístup k datovým sadám správce front v systému z/OS*

Administrátoři produktu IBM MQ for z/OS potřebují oprávnění pro přístup k datovým sadám správce front. V tomto tématu se můžete seznámit s tím, které datové sady vyžadují ochranu RACF .

Tyto datové sady zahrnují:

- Datové sady, na které odkazují CSQINP1, CSQINP2a CSQINPT v proceduře spuštěné úlohy správce front.
- Sady stránek správce front, datové sady aktivního protokolu, datové sady archivního protokolu a datové sady samozavedení (BSDS)
- Datové sady, na které odkazují knihovny CSQXLIB a CSQINPX v proceduře spuštěné úlohy inicializátoru kanálu.

Datové sady je třeba chránit tak, aby žádný neautorizovaný uživatel nespustil správce front ani nezískal přístup k žádným datům správce front. Chcete-li to provést, použijte ochranu datové sady RACF .

Autorizace pro použití aplikací IBM MQ

Když aplikace přistupují k objektům, ID uživatelů přidružená k aplikacím potřebují odpovídající oprávnění.

Aplikace mohou přistupovat k následujícím objektům produktu IBM MQ pomocí volání MQI:

- Správci front
- Fronty
- Procesy
- Seznamy názvů
- Témata

Aplikace mohou také používat příkazy PCF ke správě objektů IBM MQ . Když je příkaz PCF zpracován, používá kontext oprávnění ID uživatele, který vložil zprávu PCF.

Aplikace v tomto kontextu zahrnují aplikace napsané uživateli a dodavateli a aplikace dodávané s produktem IBM MQ for z/OS. Aplikace dodávané s produktem IBM MQ for z/OS zahrnují:

- Provozní a ovládací panely
- Obslužný program IBM MQ , CSQUTIL
- Obslužný program pro obslužnou rutinu fronty nedoručených zpráv, CSQUDLQH

Aplikace, které používají produkty IBM MQ classes for Java, IBM MQ classes for JMS, IBM MQ classes for .NETnebo klienty služby zpráv pro C/C++ a .NET , používají rozhraní MQI nepřímo.

MCA také vydávají volání MQI a ID uživatelů přidružená k MCA potřebují oprávnění pro přístup k těmto objektům produktu IBM MQ . Další informace o těchto ID uživatelů a potřebném oprávnění naleznete v části “Autorizace kanálu” na stránce 113.

V systému z/OSmohou aplikace také používat příkazy MQSC pro přístup k těmto objektům produktu IBM MQ , ale zabezpečení příkazů a zabezpečení prostředků příkazů poskytují za těchto okolností kontroly oprávnění. z/OS Další informace viz “Zabezpečení příkazů a zabezpečení prostředků příkazů v systému z/OS” na stránce 91 a “Příkazy MQSC a vstupní fronta systémových příkazů v systému z/OS” na stránce 92.

V systému IBM iMůže uživatel, který vydává příkaz CL ve skupině 2, požadovat oprávnění pro přístup k objektu IBM MQ přidruženému k příkazu. Další informace viz “Při provádění kontrol oprávnění” na stránce 93.

Při provádění kontrol oprávnění

Kontroly oprávnění se provádějí při pokusu aplikace o přístup ke správci front, frontě, procesu nebo seznamu názvů.

V systému IBM imohou být kontroly oprávnění také provedeny, když uživatel vydá příkaz CL ve skupině 2, který přistupuje k libovolným z těchto objektů IBM MQ . Kontroly se provádějí za těchto okolností:

Když se aplikace připojí ke správci front pomocí volání `MQCONN` nebo `MQCONNX` .
Správce front požádá operační systém o ID uživatele přidružené k aplikaci. Správce front poté zkontroluje, zda je ID uživatele autorizováno pro připojení k němu, a uchová ID uživatele pro budoucí kontroly.

Uživatelé se nemusí přihlašovat k produktu IBM MQ. Produkt IBM MQ předpokládá, že uživatelé jsou přihlášeni k základnímu operačnímu systému a jsou jím ověřeni.

Když aplikace otevře objekt IBM MQ pomocí volání `MQOPEN` nebo `MQPUT1`
Všechny kontroly oprávnění se provádějí při otevření objektu, ne při pozdějším přístupu. Kontroly oprávnění se například provádějí, když aplikace otevře frontu. Neprovádějí se, když aplikace vkládá zprávy do fronty nebo získává zprávy z fronty.

Když aplikace otevře objekt, uvádí typy operací, které musí s objektem provést. Aplikace může například otevřít frontu, procházet v ní zprávy, získat z ní zprávy, ale ne do ní vkládat zprávy. Pro každý typ operace správce front kontroluje, zda má ID uživatele přidružené k aplikaci oprávnění k provedení této operace.

Když aplikace otevře frontu, provedou se kontroly oprávnění vůči objektu uvedenému v poli `ObjectName` deskriptoru objektu. Pole `ObjectName` se používá ve volání `MQOPEN` nebo `MQPUT1` .

Je-li objekt alias frontou nebo definicí vzdálené fronty, kontroly oprávnění se provedou na samotném objektu. Neprovádějí se ve frontě, do které se převádí alias fronta nebo definice vzdálené fronty. To znamená, že uživatel nepotřebuje oprávnění pro přístup k němu. Omezte oprávnění k vytváření front na oprávněné uživatele. Pokud tak neučiníte, uživatelé mohou obejít běžné řízení přístupu jednoduše vytvořením aliasu.

Aplikace může explicitně odkazovat na vzdálenou frontu. Nastaví pole `ObjectName` a `ObjectQMgrName` v deskriptoru objektu na názvy vzdálené fronty a vzdáleného správce front. Kontroly oprávnění jsou prováděny pro přenosovou frontu se stejným názvem jako vzdálený správce front:

- z/OS V systému z/OSse provádí kontrola profilu fronty RACF , který odpovídá názvu vzdáleného správce front, a provádí se bez ohledu na to, zda je tato přenosová fronta definována lokálně.
- Multi V systému Multiplatformsse provádí kontrola profilu RQMNAME, který se shoduje s názvem vzdáleného správce front, pokud se používá klastrování.

Aplikace může na frontu klastru odkazovat explicitně nastavením pole `ObjectName` v deskriptoru objektu na název fronty klastru. Kontroly oprávnění se provádějí s přenosovou frontou klastru `SYSTEM.CLUSTER.TRANSMIT.QUEUE`.

Oprávnění k dynamické frontě je založeno na modelové frontě, ze které je odvozeno, ale nemusí být nutně stejné; viz poznámka 1.

ID uživatele, které správce front používá pro kontroly oprávnění, je získáno z operačního systému. ID uživatele se získá, když se aplikace připojí ke správci front. Vhodně autorizovaná aplikace může vydat volání `MQOPEN` uvádějící alternativní ID uživatele; kontroly řízení přístupu se pak provádějí na alternativním ID uživatele. Použití alternativního ID uživatele nezmění ID uživatele přidružené k aplikaci, pouze to, které se používá pro kontroly řízení přístupu.

Když se aplikace přihlásí k odběru tématu pomocí volání `MQSUB`

Když se aplikace přihlásí k odběru tématu, uvádí typ operace, kterou musí provést. Buď vytváří odběr, mění existující odběr, nebo obnovuje existující odběr bez jeho změny. Pro každý typ operace správce front kontroluje, zda má ID uživatele přidružené k aplikaci oprávnění k provedení operace.

Když se aplikace přihlásí k odběru tématu, provedou se kontroly oprávnění pro objekty témat, které se nacházejí ve stromu témat. Objekty tématu se nacházejí ve stromu témat, ve kterém byla aplikace přihlášena k odběru, nebo nad ním. Kontroly oprávnění mohou zahrnovat kontroly více než jednoho objektu tématu. ID uživatele, které správce front používá pro kontroly oprávnění, je získáno z operačního systému. ID uživatele se získá, když se aplikace připojí ke správci front.

Správce front provádí kontroly oprávnění ve frontách odběratelů, nikoli však ve spravovaných frontách.

Když aplikace odstraní trvalou dynamickou frontu pomocí volání `MQCLOSE`

Popisovač objektu zadaný ve volání `MQCLOSE` nemusí být nutně stejný jako popisovač vrácený voláním `MQOPEN` , které vytvořilo trvalou dynamickou frontu. Pokud se liší, správce front zkontroluje ID uživatele přidružené k aplikaci, která vydala volání `MQCLOSE` . Kontroluje, zda je ID uživatele autorizováno k odstranění fronty.

Když aplikace, která zavře odběr, aby jej odebrala, jej nevytvořila, je pro jeho odebrání vyžadováno příslušné oprávnění.

Když je příkaz PCF, který pracuje s objektem IBM MQ , zpracován příkazovým serverem.

Toto pravidlo zahrnuje případ, kdy příkaz PCF pracuje s objektem ověřovacích informací.

ID uživatele, které se používá pro kontroly oprávnění, je ID nalezené v poli `UserIdentifier` v deskriptoru zprávy příkazu PCF. Toto ID uživatele musí mít požadovaná oprávnění pro správce front, kde je příkaz zpracován. Ekvivalentní příkaz MQSC zapouzdřený v příkazu Escape PCF je zpracován stejným způsobem. Další informace o poli `UserIdentifier` a jeho nastavení viz “kontext zprávy” na stránce 95.

IBM i V systému IBM i, když uživatel zadá příkaz CL ve skupině 2, který pracuje s objektem IBM MQ .

Toto pravidlo zahrnuje případ, kdy CL příkaz ve skupině 2 pracuje s objektem ověřovacích informací.

Provedou se kontroly, aby se zjistilo, zda má uživatel oprávnění pracovat s objektem IBM MQ přidruženým k příkazu. Kontroly se provádějí, pokud není uživatel členem skupiny QMQMADM nebo nemá oprávnění *ALLOBJ . Požadované oprávnění závisí na typu operace, kterou příkaz provádí na objektu. Například příkaz **CHGMQMQ**, Změnit frontu MQM, vyžaduje oprávnění ke změně atributů fronty určené příkazem. Naproti tomu příkaz **DSPMQMQ**, Display MQM Queue, vyžaduje oprávnění k zobrazení atributů fronty určené příkazem.

Mnoho příkazů pracuje s více než jedním objektem. Chcete-li například zadat příkaz **DLTMQMQ**, Delete MQM Queue, jsou vyžadována následující oprávnění:

- Oprávnění pro připojení ke správci front určené příkazem
- Oprávnění k odstranění fronty uvedené příkazem

Některé příkazy vůbec nefungují na žádném objektu. V tomto případě uživatel vyžaduje pouze oprávnění IBM i k vydání jednoho z těchto příkazů. **STRMQMLSR**, Příkladem takového příkazu je spuštění modulu listener MQM.

Oprávnění alternativního uživatele

Když aplikace otevře objekt nebo se přihlásí k odběru tématu, může zadat ID uživatele pro volání MQOPEN, MQPUT1nebo MQSUB. Může požádat správce front o použití tohoto ID uživatele pro kontroly oprávnění namísto ID přidruženého k aplikaci.

Aplikace úspěšně otevře objekt pouze v případě, že jsou splněny obě následující podmínky:

- ID uživatele přidružené k aplikaci má oprávnění k dodání jiného ID uživatele pro kontroly oprávnění. O aplikaci se říká, že má *alternativní oprávnění uživatele*.
- ID uživatele zadané aplikací má oprávnění k otevření objektu pro požadované typy operací nebo k přihlášení k odběru tématu.

kontext zprávy

Kontext zprávy umožňuje aplikaci, která načte zprávu, zjistit informace o původci zprávy. Informace jsou uloženy v polích v deskriptoru zprávy a pole jsou rozdělena do tří logických částí.

Tyto části jsou následující:

kontext identity
Tato pole obsahují informace o uživateli aplikace, který vložil zprávu do fronty.

původní kontext
Tato pole obsahují informace o samotné aplikaci a o tom, kdy byla zpráva vložena do fronty.

uživatelský kontext
Tato pole obsahují vlastnosti zpráv, které mohou aplikace použít k výběru zpráv, které by měl správce front doručit.

Když aplikace vloží zprávu do fronty, může požádat správce front o vygenerování informací o kontextu ve zprávě. Toto je výchozí akce. Alternativně může určit, že pole kontextu nemají obsahovat žádné informace. ID uživatele přidružené k aplikaci nevyžaduje žádné speciální oprávnění k provedení jedné z těchto akcí.

Aplikace může nastavit pole kontextu identity ve zprávě, což správci front umožní generovat původní kontext, nebo může nastavit všechna pole kontextu. Aplikace může také předat pole kontextu identity ze zprávy, kterou načetla, do zprávy, kterou vkládá do fronty, nebo může předat všechna pole kontextu. Avšak ID uživatele přidružené k aplikaci vyžaduje oprávnění k nastavení nebo předání informací o kontextu. Aplikace určuje, že má v úmyslu nastavit nebo předat informace o kontextu, když otevře frontu, do které má vkládat zprávy, a její autorita je v tuto chvíli kontrolována.

Zde je stručný popis jednotlivých polí kontextu:

kontext identity

UserIdentifier
ID uživatele přidružené k aplikaci, která vložila zprávu. Pokud správce front nastaví toto pole, nastaví se na ID uživatele získané z operačního systému při připojení aplikace ke správci front.

AccountingToken
Informace, které lze použít k účtování za práci provedenou jako výsledek zprávy.

ApplIdentityData
Pokud má ID uživatele přidružené k aplikaci oprávnění k nastavení polí kontextu identity nebo k nastavení všech polí kontextu, může aplikace nastavit toto pole na libovolnou hodnotu související s identitou. Pokud správce front nastaví toto pole, bude prázdné.

Původní kontext

PutApplType
Typ aplikace, která vložila zprávu; například transakce CICS .

PutApplName
Název aplikace, která vložila zprávu.

PutDate
Datum, kdy byla zpráva vložena.

PutTime
Čas, kdy byla zpráva vložena.

ApplOriginData
Pokud má ID uživatele přidružené k aplikaci oprávnění nastavit všechna pole kontextu, aplikace může toto pole nastavit na libovolnou hodnotu související s původem. Pokud správce front nastaví toto pole, bude prázdné.

Uživatelský kontext

Následující hodnoty jsou podporovány pro **MQINQMP** nebo **MQSETMP**:

MQPD_USER _CONTEXT

Vlastnost je přidružena ke kontextu uživatele.

Pro nastavení vlastnosti přidružené ke kontextu uživatele pomocí volání MQSETMP není vyžadována žádná speciální autorizace.

V V7.0 nebo následném správci front je vlastnost přidružená ke kontextu uživatele uložena podle popisu pro MQOO_SAVE_ALL_CONTEXT. Operace MQPUT se zadaným parametrem MQOOO_PASS_ALL_CONTEXT způsobí zkopírování vlastnosti z uloženého kontextu do nové zprávy.

MQPD_NO_CONTEXT

Vlastnost není přidružena ke kontextu zprávy.

Nerozpoznaná hodnota je odmítnuta s hodnotou MQRC_PD_ERROR. Počáteční hodnota tohoto pole je **MQPD_NO_CONTEXT**.

Podrobný popis jednotlivých polí kontextu naleznete v tématu MQMD-Deskriptor zpráv. Další informace o použití kontextu zprávy viz Kontext zprávy.

IBM i ALW *Oprávnění pro práci s objekty IBM MQ na systémech* IBM i *IBM i , AIX, Linux, and Windows*

Komponenta služby autorizace poskytovaná s produktem IBM MQ se nazývá *správce oprávnění k objektu* (OAM). Poskytuje řízení přístupu prostřednictvím ověření a kontrol autorizace.

Ověření.
Kontrola ověření prováděná modulem OAM poskytovaným s produktem IBM MQ je základní a provádí se pouze za specifických okolností. Není určen ke splnění přísných požadavků očekávaných ve vysoce zabezpečeném prostředí.

OAM provádí svou kontrolu ověření, když se aplikace připojí ke správci front, a platí následující podmínky:

- pokud byla struktura MQCSP dodána připojující se aplikací a
- Atributu *AuthenticationType* ve struktuře MQCSP je přiřazena hodnota MQCSP_AUTH_USER_ID_AND_PWD a
- Hodnota CHCKLOCL nebo CHKCCLNT v konfigurovaném objektu AUTHINFO není 'NONE'

Kroky ověření v OAM ověřují heslo pomocí služeb operačního systému, které mohly být nakonfigurovány tak, aby prováděly další kontroly, například aby zajistily, že jméno uživatele nemělo příliš mnoho nesprávných pokusů o testování hesla.

Pokud napíšete novou komponentu služby autorizace nebo ji získáte od dodavatele, je možné použít alternativní mechanizmy ověřování.

Oprávnění.
Kontroly autorizace jsou komplexní a jsou určeny ke splnění většiny běžných požadavků.

Kontroly autorizace se provádějí, když aplikace vydá volání MQI pro přístup ke správci front, frontě, procesu, tématu nebo seznamu názvů. Provádějí se také jindy, například při provádění příkazu příkazovým serverem.

V systémech IBM i IBM i , AIX, Linux, and Windows poskytuje *autorizační služba* řízení přístupu, když aplikace vydá volání MQI pro přístup k objektu IBM MQ , který je správcem front, frontou, procesem, tématem nebo seznamem názvů. To zahrnuje kontroly alternativního oprávnění uživatele a oprávnění k nastavení nebo předání informací o kontextu.

Windows V systému Windows poskytuje modul OAM členům skupiny administrátorů oprávnění pro přístup ke všem objektům produktu IBM MQ , a to i v případě, že je povolen modul UAC. Na systémech Windows má navíc účet SYSTEM úplný přístup k prostředkům IBM MQ .

Autorizační služba také poskytuje kontroly oprávnění, když příkaz PCF pracuje na jednom z těchto objektů IBM MQ nebo na objektu ověřovacích informací. Ekvivalentní příkaz MQSC zapouzdřený v příkazu Escape PCF je zpracován stejným způsobem.

IBM i V systému IBM i platí, že pokud uživatel není členem skupiny QMQMADM nebo nemá oprávnění *ALLOBJ, poskytuje autorizační služba také kontroly oprávnění v případě, že uživatel vydá příkaz CL ve skupině 2, který pracuje s libovolným z těchto objektů IBM MQ nebo s objektem ověřovacích informací.

Autorizační služba je *instalovatelná služba*, což znamená, že je implementována jednou nebo více *instalovatelnými komponentami služby*. Každá komponenta je vyvolána pomocí dokumentovaného rozhraní. To umožňuje uživatelům a dodavatelům poskytovat komponenty pro rozšíření nebo nahrazení komponent poskytovaných produkty IBM MQ .

Komponenta služby autorizace poskytovaná s produktem IBM MQ se nazývá OAM (Object Authority Manager). Modul OAM je automaticky povolen pro každého vytvořeného správce front.

OAM udržuje seznam přístupových práv (ACL) pro každý objekt IBM MQ , ke kterému řídí přístup. V systémech AIX and Linux se v seznamu ACL mohou objevit pouze ID skupin. To znamená, že všichni členové skupiny mají stejná oprávnění. V systémech IBM i IBM i a Windows se v seznamu přístupových práv mohou objevit ID uživatelů i ID skupin. To znamená, že oprávnění lze udělit jednotlivým uživatelům a skupinám.

Omezení na 12 znaků platí jak pro skupinu, tak pro ID uživatele. Platformy UNIX obecně omezují délku ID uživatele na 12 znaků. AIX a Linux zvýšily tento limit, ale IBM MQ nadále dodržuje omezení na 12 znaků na všech platformách UNIX . Pokud použijete ID uživatele delší než 12 znaků, produkt IBM MQ jej nahradí hodnotou "UNKNOWN". Nedefinujte ID uživatele s hodnotou "UNKNOWN".

OAM může ověřit uživatele a změnit odpovídající pole kontextu identity. Tuto možnost povolíte určením struktury parametrů zabezpečení připojení (MQCSP) ve volání MQCONNX. Struktura je předána funkci OAM Authenticate User (MQZ_AUTHENTICATE_USER), která nastavuje příslušná pole kontextu identity.

Pokud se jedná o připojení MQCONNX z klienta IBM MQ , jsou informace v MQCSP přeneseny do správce front, ke kterému se klient připojuje prostřednictvím připojení klienta a kanálu připojení serveru. Jsou-li v daném kanálu definovány uživatelské procedury zabezpečení, je protokol MQCSP předán do každé uživatelské procedury zabezpečení a může být uživatelskou procedurou změněn. Uživatelské procedury zabezpečení mohou také vytvořit MQCSP. Další podrobnosti o použití uživatelských procedur zabezpečení v tomto kontextu naleznete v tématu Programy uživatelských procedur zabezpečení kanálu.

Varování: V některých případech bude heslo ve struktuře MQCSP pro klientskou aplikaci odesláno v síti jako prostý text. Chcete-li se ujistit, že jsou hesla aplikací klienta řádně chráněna, prohlédněte si téma IBM MQOchrana hesel CSP.

V systémech AIX, Linux, and Windows řídicí příkaz **setmqaut** uděluje a odvolává oprávnění a používá se k údržbě seznamů ACL. Například příkaz:

```
setmqaut -m JUPITER -t queue -n MOON.EUROPA -g VOYAGER +browse +get
```

umožňuje členům skupiny VOYAGER procházet zprávy ve frontě MOON.EUROPA vlastněný správcem front JUPITER. Umožňuje členům také získat zprávy z fronty. Chcete-li později tato oprávnění odvolat, zadejte následující příkaz:

```
setmqaut -m JUPITER -t queue -n MOON.EUROPA -g VOYAGER -browse -get
```

Příkaz:

```
setmqaut -m JUPITER -t queue -n MOON.* -g VOYAGER +put
```

umožňuje členům skupiny VOYAGER vkládat zprávy do libovolné fronty s názvem, který začíná znaky MOON.. MOON.* je název generického profilu.*Generický profil* vám umožňuje udělit oprávnění pro sadu objektů pomocí jediného příkazu **setmqaut** .

Řídicí příkaz **dspmqaut** je k dispozici pro zobrazení aktuálních oprávnění, která má uživatel nebo skupina pro uvedený objekt.Řídicí příkaz **dmpmqaut** je také k dispozici pro zobrazení aktuálních oprávnění přidružených ke generickým profilům.

IBM i V systému IBM ipoužívá administrátor příkaz CL GRTMQMAUT k udělení oprávnění a příkaz CL RVKMQMAUT k odvolání oprávnění. Generické profily mohou být také použity.Například příkaz CL:

```
GRTMQMAUT MQMNAME(JUPITER) OBJTYPE(*Q) OBJ('MOON.*') USER(VOYAGER) AUT(*PUT)
```

poskytuje stejnou funkci jako předchozí příklad příkazu **setmqaut** ; umožňuje členům skupiny VOYAGER vkládat zprávy do libovolné fronty s názvem, který začíná znaky MOON.

IBM i CL příkaz DSPMQMAUT zobrazí aktuální oprávnění, která má uživatel nebo skupina pro uvedený objekt. CL příkazy WRKMQMAUT a WRKMQMAUTD jsou také k dispozici pro práci s aktuálními oprávněními přidruženými k objektům a generickým profilům.

Pokud nechcete žádné kontroly oprávnění, například v testovacím prostředí, můžete zakázat OAM.

Multi *Použití PCF pro přístup k příkazům OAM*
Na systémech IBM i, AIX, Linux, and Windows můžete použít příkazy PCF pro přístup k příkazům administrace OAM.

Příkazy PCF a jejich ekvivalentní příkazy OAM jsou následující:

Tabulka 8. Příkazy PCF a jejich ekvivalentní příkazy OAM

Příkaz PCF	**Příkaz OAM**
Zjistit záznamy oprávnění	dmpmqaut

Tabulka 8. Příkazy PCF a jejich ekvivalentní příkazy OAM (pokračování)	
Příkaz PCF	**Příkaz OAM**
Zjistit oprávnění k entitě	dspmqaut
Nastavit záznam oprávnění	setmqaut
Odstranit záznam oprávnění	setmqaut s volbou -remove

Příkazy **setmqaut** a **dmpmqaut** jsou omezeny na členy skupiny mqm. Ekvivalentní příkazy PCF mohou provádět uživatelé v libovolné skupině, kterým byla udělena oprávnění dsp a chg pro správce front.

Další informace o použití těchto příkazů naleznete v tématu Úvod do programovatelných formátů příkazů.

z/OS *Oprávnění pro práci s objekty IBM MQ na systému z/OS*

V systému z/OSexistuje sedm kategorií kontroly oprávnění přidružených k voláním rozhraní MQI. Musíte definovat určité profily RACF a udělit k nim odpovídající přístup. Pomocí profilu *RESLEVEL* můžete řídit, kolik ID uživatelů je kontrolováno.

Sedm kategorií kontroly oprávnění přidružených k voláním rozhraní MQI:

Zabezpečení připojení
Kontroly oprávnění, které se provádějí při připojení aplikace ke správci front

Zabezpečení fronty
Kontroly oprávnění, které se provádějí, když aplikace otevře frontu nebo odstraní trvalou dynamickou frontu.

Zabezpečení procesů
Kontroly oprávnění, které se provádějí, když aplikace otevře objekt procesu

Zabezpečení seznamu názvů
Kontroly oprávnění, které se provádějí, když aplikace otevře objekt seznamu názvů

alternativní zabezpečení uživatele
Kontroly oprávnění, které se provádějí, když aplikace požaduje alternativní oprávnění uživatele při otevírání objektu

zabezpečení kontextu
Kontroly oprávnění, které se provádějí, když aplikace otevře frontu, a uvádí, že zamýšlí nastavit nebo předat informace o kontextu ve zprávách, které vkládá do fronty.

Zabezpečení tématu
Kontroly oprávnění, které se provádějí, když aplikace otevře téma

Každá kategorie kontroly oprávnění je implementována stejným způsobem, jakým je implementováno zabezpečení příkazů a zabezpečení prostředků příkazů. Musíte definovat určité profily RACF a poskytnout potřebným skupinám a ID uživatelů přístup k těmto profilům na požadovaných úrovních. V případě zabezpečení fronty úroveň přístupu určuje typy operací, které může aplikace ve frontě provádět. V případě zabezpečení kontextu úroveň přístupu určuje, zda může aplikace:

- Předat všechna pole kontextu
- Předat všechna pole kontextu a nastavit pole kontextu identity
- Předat a nastavit všechna pole kontextu

Každou kategorii kontroly oprávnění lze zapnout nebo vypnout definováním profilů přepínače.

Všechny kategorie, s výjimkou zabezpečení připojení, jsou souhrnně označovány jako *zabezpečení prostředků rozhraní API*.

Při výchozím nastavení je při provádění kontroly zabezpečení prostředků rozhraní API v důsledku volání MQI z aplikace používající dávkové připojení kontrolováno pouze jedno ID uživatele. Je-li kontrola provedena v důsledku volání MQI z aplikace CICS nebo IMS nebo z inicializátoru kanálu, jsou zkontrolována dvě ID uživatelů.

Definováním *profilu RESLEVEL*však můžete řídit, zda jsou kontrolována nulová, jedna nebo dvě ID uživatelů. Počet kontrolovaných ID uživatelů je určen ID uživatele přidruženým k typu připojení, když se aplikace připojí ke správci front a úroveň přístupu, kterou má ID uživatele k profilu RESLEVEL. ID uživatele přidružené ke každému typu připojení je:

- ID uživatele připojující se úlohy pro dávková připojení
- ID uživatele adresního prostoru CICS pro připojení CICS
- ID uživatele adresního prostoru oblasti IMS pro připojení IMS
- ID uživatele adresního prostoru inicializátoru kanálu pro připojení inicializátoru kanálu

Další informace o oprávnění pracovat s objekty IBM MQ v systému z/OSviz “Oprávnění ke správě IBM MQ v systému z/OS” na stránce 90.

Zabezpečení pro vzdálený systém zpráv

Tato část se zabývá aspekty zabezpečení vzdáleného systému zpráv.

Musíte poskytnout uživatelům oprávnění k používání zařízení IBM MQ . To je uspořádáno podle akcí, které mají být provedeny s ohledem na objekty a definice. Příklad:

- Autorizovaní uživatelé mohou spouštět a zastavovat správce front.
- Aplikace se musí připojit ke správci front a musí mít oprávnění používat fronty.
- Kanály zpráv musí být vytvořeny a řízeny autorizovanými uživateli.
- Objekty jsou uchovávány v knihovnách a přístup k těmto knihovnám může být omezen

Agent kanálu zpráv na vzdáleném serveru musí zkontrolovat, zda doručovaná zpráva pochází od uživatele s oprávněním tak učinit na tomto vzdáleném serveru. Kromě toho, protože adaptéry MCA lze spustit vzdáleně, může být nutné ověřit, že vzdálené procesy, které se pokoušejí spustit vaše adaptéry MCA, jsou k tomu autorizovány. Existují čtyři možné způsoby, jak se s tím vypořádat:

1. Odpovídajícím způsobem použijte atribut PutAuthority definice kanálu RCVR, RQSTR nebo CLUSRCVR k řízení toho, který uživatel se používá pro kontroly autorizace v době, kdy jsou příchozí zprávy vkládány do front. Viz popis příkazu DEFINE CHANNEL v příručce MQSC Command Reference.
2. Implementujte záznamy ověřování kanálu, chcete-li odmítnout nežádoucí pokusy o připojení nebo nastavit hodnotu MCAUSER na základě následujících údajů: adresa IP vzdáleného systému, ID vzdáleného uživatele, zadaný rozlišující název subjektu TLS nebo název vzdáleného správce front.
3. Implementujte kontrolu zabezpečení *uživatelské procedury* , abyste se ujistili, že je odpovídající kanál zpráv autorizován. Zabezpečení instalace hostující odpovídající kanál zajišťuje, že všichni uživatelé jsou řádně autorizováni, takže nemusíte kontrolovat jednotlivé zprávy.
4. Implementujte zpracování zpráv *uživatelské procedury* , abyste se ujistili, že jsou jednotlivé zprávy prověřeny pro autorizaci.

IBM i *Zabezpečení objektů IBM MQ for IBM i*

Tato část se zabývá aspekty zabezpečení vzdáleného systému zpráv.

Chcete-li využívat zařízení IBM MQ for IBM i , musíte uživatelům poskytnout oprávnění. Toto oprávnění je uspořádáno podle akcí, které mají být provedeny s ohledem na objekty a definice. Příklad:

- Autorizovaní uživatelé mohou spouštět a zastavovat správce front.
- Aplikace se musí připojit ke správci front a mají oprávnění používat fronty.
- Kanály zpráv musí být vytvořeny a řízeny autorizovanými uživateli.

Agent kanálu zpráv na vzdáleném serveru musí zkontrolovat, zda doručovaná zpráva pochází od uživatele s oprávněním k zobrazení zprávy na tomto vzdáleném serveru. Kromě toho, protože adaptéry MCA lze spustit vzdáleně, může být nutné ověřit, že vzdálené procesy, které se pokoušejí spustit vaše adaptéry MCA, jsou k tomu autorizovány. Existují čtyři možné způsoby, jak se s tím vypořádat:

- V definici kanálu platí, že zprávy musí obsahovat přijatelnou autoritu *kontextu* , jinak budou vyřazeny.

- Implementujte záznamy ověřování kanálu, chcete-li odmítnout nežádoucí pokusy o připojení nebo nastavit hodnotu MCAUSER na základě jedné z následujících možností: adresa IP vzdáleného systému, ID vzdáleného uživatele, poskytnutý rozlišující název TLS (DN) nebo název vzdáleného správce front.
- Implementujte kontrolu zabezpečení uživatelské procedury, abyste se ujistili, že je odpovídající kanál zpráv autorizován. Zabezpečení instalace hostující odpovídající kanál zajišťuje, že všichni uživatelé jsou řádně autorizováni, takže nemusíte kontrolovat jednotlivé zprávy.
- Implementujte zpracování zpráv uživatelské procedury, abyste se ujistili, že jsou jednotlivé zprávy prověřeny pro autorizaci.

Zde je několik faktů o tom, jak IBM MQ for IBM i funguje zabezpečení:

- Uživatelé jsou identifikováni a ověřeni produktem IBM i.
- Služby správce front vyvolané aplikacemi jsou spuštěny s oprávněním profilu uživatele správce front, ale v procesu uživatele.
- Služby správce front vyvolané příkazy uživatele jsou spouštěny s oprávněním profilu uživatele správce front.

Linux AIX *Zabezpečení objektů na systému AIX and Linux*

Uživatelé s oprávněními administrátora musí být součástí skupiny mqm ve vašem systému (včetně uživatele root), pokud bude toto ID používat příkazy administrace IBM MQ .

Vždy byste měli spustit příkaz amqcrsta jako ID uživatele "mqm".

ID uživatelů v systému AIX and Linux

Správce front převede všechny identifikátory uživatelů s velkými i smíšenými písmeny na malá písmena. Správce front poté vloží identifikátory uživatelů do kontextové části zprávy nebo zkontroluje jejich autorizaci. Autorizace jsou proto založeny pouze na malých identifikátorech.

Windows *Zabezpečení objektů v systémech Windows*

Administrativní uživatelé musí být součástí skupiny mqm i skupiny administrátorů na systémech Windows , pokud bude toto ID používat příkazy administrace IBM MQ .

ID uživatelů na systémech Windows

V systémech Windows *, pokud není instalována žádná uživatelská procedura pro zprávy*, převede správce front všechny identifikátory uživatelů s velkými nebo smíšenými písmeny na malá písmena. Správce front poté vloží identifikátory uživatelů do kontextové části zprávy nebo zkontroluje jejich autorizaci. Autorizace jsou proto založeny pouze na malých identifikátorech.

ID uživatelů v různých systémech

Jiné platformy než systémy AIX, Linux, and Windows používají pro ID uživatelů ve zprávách velká písmena. Chcete-li povolit systémům AIX, Linux, and Windows používat ve zprávách malá písmena ID uživatelů, musí agent kanálu zpráv (MCA) provést odpovídající převody abecedních znaků.

Chcete-li povolit systémům AIX, Linux, and Windows používat ve zprávách malá písmena ID uživatelů, agent MCA (message channel agent) provádí na těchto platformách následující převody:

Na odesílajícím konci
Abecední znaky ve všech ID uživatelů jsou převedeny na velká písmena, pokud není instalována žádná uživatelská procedura pro zprávy.

Na přijímacím konci
Abecední znaky ve všech ID uživatelů jsou převedeny na malá písmena, pokud není nainstalována žádná uživatelská procedura pro zprávy.

Automatické převody se neprovádějí, pokud v systému AIX, Linux, and Windows zadáte uživatelskou proceduru pro zprávy z jiného důvodu.

Použití vlastní autorizační služby

Produkt IBM MQ dodává instalovatelnou autorizační službu. Můžete zvolit instalaci alternativní služby.

Komponenta služby autorizace dodávaná s produktem IBM MQ se nazývá OAM (Object Authority Manager). Pokud modul OAM nedodává potřebné prostředky autorizace, můžete vytvořit vlastní komponentu služby autorizace. Instalovatelné servisní funkce, které musí být implementovány komponentou služby autorizace, jsou popsány v části Referenční informace o rozhraní instalovatelných služeb.

Řízení přístupu pro klienty

Řízení přístupu je založeno na ID uživatelů. Pro správu může existovat mnoho ID uživatelů a ID uživatelů mohou být v různých formátech. Vlastnost kanálu připojení serveru MCAUSER můžete nastavit na speciální hodnotu ID uživatele pro použití klienty.

Řízení přístupu v produktu IBM MQ je založeno na ID uživatelů. ID uživatele procesu, který provádí volání MQI, se obvykle používá. V případě klientů MQI produktu MQ provádí agent MCA připojení serveru volání MQI jménem klientů MQI produktu MQ . Můžete vybrat alternativní ID uživatele pro agenta MCA připojení serveru, který má být použit pro volání MQI. Alternativní ID uživatele může být přidruženo buď k pracovní stanici klienta, nebo k čemukoli, co se rozhodnete pro uspořádání a řízení přístupu klientů. ID uživatele musí mít na serveru přidělena potřebná oprávnění k volání MQI. Výběr alternativního ID uživatele je vhodnější k tomu, aby klienti mohli provádět volání MQI s oprávněním MCA připojení serveru.

Tabulka 9. ID uživatele použité kanálem připojení serveru

Jméno uživatele	Při použití
ID uživatele, které je nastaveno uživatelskou procedurou pro zabezpečení zprávy	Používá se, pokud není blokováno pravidlem **CHLAUTH TYPE(BLOCKUSER)** . Další informace viz následující část “Nastavení ID uživatele v uživatelské proceduře zabezpečení” na stránce 103 .
ID uživatele, které je nastaveno pravidlem CHLAUTH	Používá se, pokud není přepsáno uživatelskou procedurou pro zabezpečení. Další informace viz Záznamy ověření kanálu .
ID uživatele definované v atributu **MCAUSER** v definici kanálu SVRCONN	Používá se, pokud není přepsáno uživatelskou procedurou pro zabezpečení nebo pravidlem CHLAUTH.
ID uživatele, které pochází z klientského počítače	Používá se, když není nastaveno žádné ID uživatele jinými prostředky.
ID uživatele, který spustil kanál připojení serveru	Používá se, když není nastaveno žádné ID uživatele jinými prostředky a není zadáno žádné ID uživatele klienta. Další informace viz následující část “ID uživatele, který spouští program kanálu” na stránce 103 .

Vzhledem k tomu, že agent MCA připojení serveru provádí volání MQI jménem vzdálených uživatelů, je důležité vzít v úvahu důsledky volání MQI pro připojení serveru MCA vydávající volání MQI jménem vzdálených klientů a způsob správy přístupu potenciálně velkého počtu uživatelů.

- Jedním z přístupů je, aby agent MCA připojení serveru vydal volání MQI s vlastním oprávněním. Ale pozor, je obvykle nežádoucí, aby MCA připojení serveru s jeho výkonnými přístupovými schopnostmi vydával volání MQI jménem uživatelů klienta.
- Dalším přístupem je použití ID uživatele, které plyne z klienta. Agent MCA připojení serveru může provádět volání MQI s použitím přístupových schopností ID uživatele klienta. Tento přístup představuje řadu otázek, které je třeba zvážit:

1. Existují různé formáty pro ID uživatele na různých platformách. To někdy způsobí problémy, pokud se formát ID uživatele na klientovi liší od přijatelných formátů na serveru.
2. Potenciálně existuje mnoho klientů s různými a měnícími se ID uživatelů. ID musí být definována a spravována na serveru.
3. Má být ID uživatele důvěryhodné? Z klienta může proudit libovolné ID uživatele, nikoli nutně ID přihlášeného uživatele. Klient může například směnit ID s úplným oprávněním `mqm` , které bylo z bezpečnostních důvodů záměrně definováno pouze na serveru.

- Upřednostňovaným přístupem je definovat tokeny identifikace klienta na serveru, a omezit tak schopnosti aplikací připojených ke klientovi. To se obvykle provádí nastavením vlastnosti kanálu připojení serveru MCAUSER na speciální hodnotu ID uživatele, kterou mají používat klienti, a definováním několika ID pro použití klienty s jinou úrovní autorizace na serveru.

Nastavení ID uživatele v uživatelské proceduře zabezpečení

Pro systém IBM MQ MQI clientsje proces, který vyvolává volání MQI, MCA připojení serveru. ID uživatele použité agentem MCA připojení serveru je obsaženo v polích `MCAUserIdentifier` nebo `LongMCAUserIdentifier` disku MQCD. Obsah těchto polí se nastavuje pomocí:

- Jakékoli hodnoty nastavené pomocí uživatelských procedur zabezpečení
- ID uživatele z klienta
- MCAUSER (v definici kanálu připojení serveru)

Uživatelská procedura zabezpečení může při vyvolání přepsat hodnoty, které jsou pro ni viditelné.

- Pokud je atribut MCAUSER kanálu připojení serveru nastaven na neprázdný, použije se hodnota MCAUSER.
- Pokud je atribut MCAUSER kanálu připojení serveru prázdný, použije se ID uživatele přijaté od klienta.
- Pokud je atribut MCAUSER kanálu připojení serveru prázdný a z klienta není přijato žádné ID uživatele, použije se ID uživatele, který spustil kanál připojení serveru.

Klient IBM MQ nesměrovává deklarovaná ID uživatele na server, když se používá uživatelská procedura zabezpečení na straně klienta.

ID uživatele, který spouští program kanálu

Když jsou pole ID uživatele odvozena od ID uživatele, který spustil kanál připojení serveru, použije se následující hodnota:

- z/OS V případě systému z/OSse jedná o ID uživatele přiřazené úloze spuštěné inicializátorem kanálu v tabulce spuštěných procedur z/OS .
- Pro protokol TCP/IP (jiný než z/OS) se jedná o ID uživatele z položky `inetd.conf` nebo ID uživatele, který spustil modul listener.
- Pro SNA (jiný než z/OS) se jedná o ID uživatele ze záznamu serveru SNA nebo (pokud neexistuje) příchozí požadavek na připojení nebo ID uživatele, který spustil modul listener.
- U protokolů NetBIOS a SPX ID uživatele, který spustil modul listener.

Pokud existují nějaké definice kanálu připojení serveru, které mají atribut MCAUSER nastavený na prázdnou hodnotu, klienti mohou tuto definici kanálu použít pro připojení ke správci front s přístupovým oprávněním určeným identifikátorem uživatele dodaným klientem. Může se jednat o bezpečnostní riziko, pokud systém, na kterém je spuštěn správce front, umožňuje neautorizovaná síťová připojení. Výchozí kanál připojení serveru IBM MQ (SYSTEM.DEF.SVRCONN) má atribut MCAUSER nastavený na prázdnou hodnotu. Chcete-li zabránit neoprávněnému přístupu, aktualizujte atribut MCAUSER výchozí definice pomocí ID uživatele, které nemá přístup k objektům produktu IBM MQ MQ .

ID uživatelů v případě

Když definujete kanál s parametrem `runmqsc`, změní se atribut MCAUSER na velká písmena, pokud není ID uživatele obsaženo v apostrofech.

ALW U serverů v systému AIX, Linux, and Windowsse obsah pole `MCAUserIdentifier` , které je přijato od klienta, změní na malá písmena.

IBM i Pro servery v systému IBM ise obsah pole `LongMCAUserIdentifier` , které je přijato od klienta, změní na velká písmena.

Linux AIX U serverů na systémech AIX and Linux se obsah pole `LongMCAUserIdentifier` , které je přijato od klienta, změní na malá písmena.

Standardně je ID uživatele, které je předáno při použití aplikace vazby IBM MQ JMS , ID uživatele pro prostředí JVM, na kterém je aplikace spuštěna.

Je také možné předat ID uživatele pomocí metody `createQueueConnection` .

Důvěrnost plánování

Naplánujte, jak udržet vaše data v tajnosti.

Důvěrnost můžete implementovat na úrovni aplikace nebo na úrovni odkazu. Můžete zvolit použití TLS, v takovém případě musíte naplánovat použití digitálních certifikátů. Můžete také použít programy výstupních kanálů, pokud standardní zařízení nesplňují vaše požadavky.

Související pojmy

“Porovnání zabezpečení na úrovni propojení a zabezpečení na úrovni aplikace” na stránce 104
Toto téma obsahuje informace o různých aspektech zabezpečení na úrovni odkazů a zabezpečení na úrovni aplikací a porovnává tyto dvě úrovně zabezpečení.

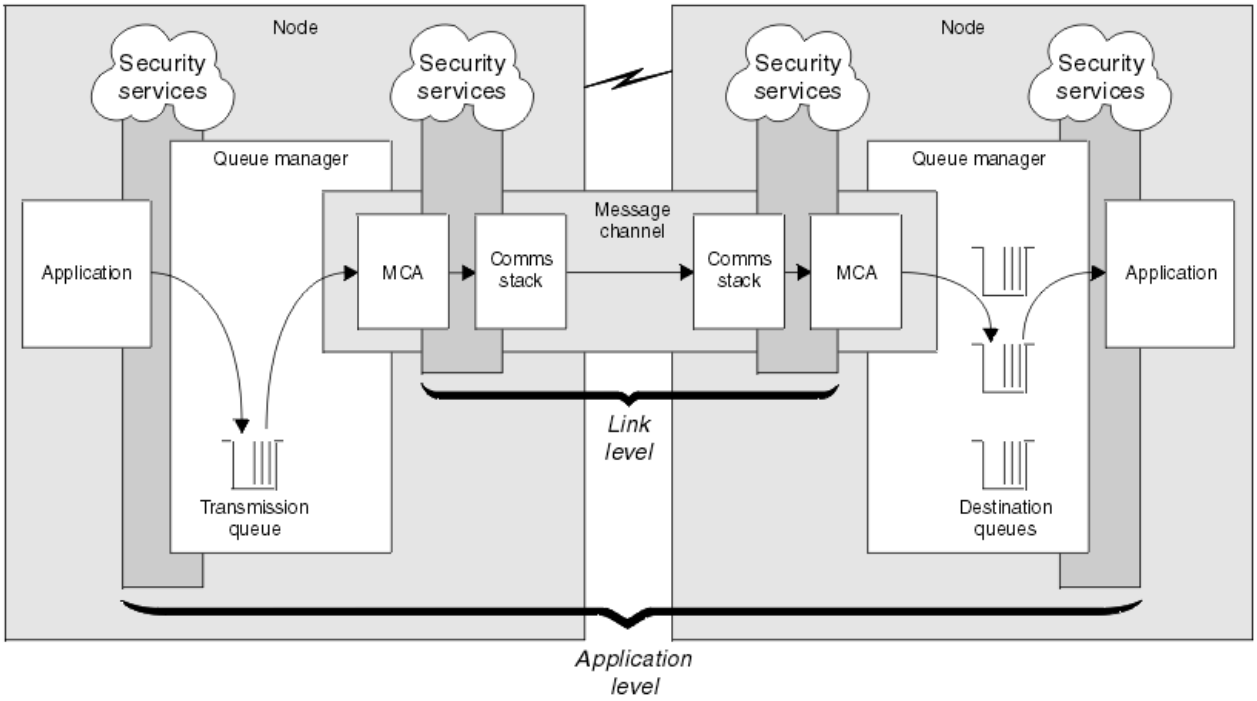
“Uživatelské programy kanálu” na stránce 109
Programy uživatelské procedury kanálu jsou programy, které jsou volány na definovaných místech v posloupnosti zpracování MCA. Uživatelé a dodavatelé mohou psát své vlastní programy výstupních kanálů. Některé jsou dodávány společností IBM.

“Ochrana kanálů pomocí SSL/TLS” na stránce 116
Podpora TLS v produktu IBM MQ používá objekt ověřovacích informací správce front a různé příkazy MQSC. Musíte také zvážit použití digitálních certifikátů.

Porovnání zabezpečení na úrovni propojení a zabezpečení na úrovni aplikace

Toto téma obsahuje informace o různých aspektech zabezpečení na úrovni odkazů a zabezpečení na úrovni aplikací a porovnává tyto dvě úrovně zabezpečení.

Úroveň propojení a úroveň zabezpečení aplikace jsou znázorněny v souboru Obrázek 10 na stránce 105.



Obrázek 10. Zabezpečení na úrovni propojení a zabezpečení na úrovni aplikace

Ochrana zpráv ve frontách

Zabezpečení na úrovni propojení může chránit zprávy během jejich přenosu z jednoho správce front do jiného. Zvláště důležité je, když jsou zprávy přenášeny přes nezabezpečenou síť. Nemůže však chránit zprávy v době, kdy jsou uloženy ve frontách ve zdrojovém správci front, cílovém správci front nebo zprostředkujícím správci front.

z/OS Šifrování datové sady z/OS může poskytnout určitou ochranu zpráv uložených ve frontách, ale pouze pro data v klidu v lokálním správci front. Viz část důvěrnost pro data v klidu na systému IBM MQ for z/OS se šifrováním datové sady. Další informace viz.

Zabezpečení na úrovni aplikace může podle porovnání chránit zprávy, zatímco jsou uloženy ve frontách, a platí i v případě, že není použito distribuované řazení do front. Jedná se o hlavní rozdíl mezi zabezpečením na úrovni propojení a zabezpečením na úrovni aplikace a je znázorněn v části Obrázek 10 na stránce 105.

Správci front, kteří nejsou spuštěni v řízených a důvěryhodných prostředích

Pokud je správce front spuštěn v řízeném a důvěryhodném prostředí, mohou být mechanizmy řízení přístupu poskytované produktem IBM MQ považovány za dostatečné pro ochranu zpráv uložených ve frontách. To platí zejména v případě, že je zapojeno pouze lokální řazení do fronty a zprávy nikdy neopouštějí správce front. Zabezpečení na úrovni aplikace v tomto případě může být považováno za zbytečné.

Zabezpečení na úrovni aplikace může být považováno za nadbytečné také v případě, že jsou zprávy přenášeny do jiného správce front, který je také spuštěn v řízeném a důvěryhodném prostředí, nebo jsou přijímány od takového správce front. Potřeba zabezpečení na úrovni aplikace se zvyšuje při přenosu zpráv do správce front, který není spuštěn v řízeném a důvěryhodném prostředí, nebo při jejich příjmu ze správce front.

Rozdíly v nákladech

Zabezpečení na úrovni aplikace může stát více než jen zabezpečení na úrovni propojení, pokud jde o administraci a výkon.

Náklady na administraci budou pravděpodobně vyšší, protože existuje potenciálně více omezení pro konfiguraci a údržbu. Můžete například zajistit, aby konkrétní uživatel odesílal pouze určité typy zpráv a odesílal zprávy pouze do určitých míst určení. Naopak, možná budete muset zajistit, aby konkrétní uživatel přijímal pouze určité typy zpráv a přijímal zprávy pouze z určitých zdrojů. Místo správy služeb zabezpečení na úrovni propojení v jednom kanálu zpráv může být nutné konfigurovat a udržovat pravidla pro každou dvojici uživatelů, kteří si vyměňují zprávy v rámci tohoto kanálu.

Pokud jsou služby zabezpečení vyvolány při každém vložení nebo získání zprávy aplikací, může to mít vliv na výkon.

Organizace mají tendenci nejprve zvážit zabezpečení na úrovni propojení, protože může být snazší jej implementovat. Zvažují zabezpečení na úrovni aplikace, pokud zjistí, že zabezpečení na úrovni odkazu nesplňuje všechny jejich požadavky.

Dostupnost komponent

Obecně v distribuovaném prostředí služba zabezpečení vyžaduje komponentu alespoň na dvou systémech. Zpráva může být například zašifrována na jednom systému a dešifrována na jiném systému. To platí jak pro zabezpečení na úrovni propojení, tak pro zabezpečení na úrovni aplikace.

V heterogenním prostředí s různými používanými platformami, z nichž každá má různé úrovně funkce zabezpečení, nemusí být požadované komponenty služby zabezpečení k dispozici pro každou platformu, na které jsou potřebné, a ve formě, která je snadno použitelná. Jedná se pravděpodobně spíše o problém zabezpečení na úrovni aplikace než zabezpečení na úrovni propojení, zejména pokud máte v úmyslu poskytnout vlastní zabezpečení na úrovni aplikace nákupem komponent z různých zdrojů.

Zprávy ve frontě nedoručených zpráv

Pokud je zpráva chráněna zabezpečením na úrovni aplikace, může dojít k problému, pokud z nějakého důvodu zpráva nedosáhne svého cíle a je vložena do fronty nedoručených zpráv. Pokud nemůžete zjistit, jak zpracovat zprávu z informací v deskriptoru zprávy a záhlaví nedoručených zpráv, možná budete muset zkontrolovat obsah dat aplikace. Tuto operaci nelze provést, pokud jsou data aplikace šifrována a dešifrovat je může pouze zamýšlený příjemce.

Jaké zabezpečení na úrovni aplikace nemůže provádět

Zabezpečení na úrovni aplikace není úplným řešením. I v případě, že implementujete zabezpečení na úrovni aplikace, můžete i nadále vyžadovat některé služby zabezpečení na úrovni propojení. Příklad:

- Při spuštění kanálu může být vzájemné ověření obou MCA stále požadavkem. To lze provést pouze pomocí služby zabezpečení na úrovni propojení.
- Zabezpečení na úrovni aplikace nemůže chránit záhlaví přenosové fronty MQXQH, které obsahuje vložený deskriptor zprávy. Nemůže také chránit data v jiných tocích protokolu kanálu IBM MQ než v datech zprávy. Tuto ochranu může poskytovat pouze zabezpečení na úrovni propojení.
- Jsou-li služby zabezpečení na úrovni aplikace vyvolány na konci serveru kanálu MQI, nemohou tyto služby chránit parametry volání MQI odesílaných prostřednictvím kanálu. Konkrétně jsou data aplikace ve volání MQPUT, MQPUT1nebo MQGET nechráněná. V tomto případě může ochranu poskytnout pouze zabezpečení na úrovni propojení.

zabezpečení na úrovni odkazů

Zabezpečení na úrovni spoje odkazuje na ty služby zabezpečení, které jsou přímo či nepřímo vyvolávány agentem MCA, komunikačním subsystémem nebo jejich kombinací.

Zabezpečení na úrovni propojení je znázorněno na obrázku Obrázek 10 na stránce 105.

Zde je několik příkladů služeb zabezpečení na úrovni odkazů:

- Agent MCA na každém konci kanálu zpráv může ověřit svého partnera. To se provede při spuštění kanálu a navázání komunikačního připojení, ale před tím, než se spustí tok zpráv. Pokud se ověření na

obou koncích nezdaří, kanál se zavře a nebudou přenášeny žádné zprávy. Toto je příklad identifikační a ověřovací služby.

- Zprávu lze šifrovat na odesílajícím konci kanálu a dešifrovat na přijímajícím konci. Toto je příklad služby důvěrnosti.
- Zprávu lze zkontrolovat na přijímacím konci kanálu, aby se zjistilo, zda byl její obsah záměrně upraven, když byl přenášen po síti. Toto je příklad služby integrity dat.

Zabezpečení na úrovni propojení poskytované produktem IBM MQ

Primárním prostředkem zajištění důvěrnosti a integrity dat v produktu IBM MQ je použití TLS. Další informace o použití TLS v IBM MQviz “Protokoly zabezpečení TLS v adresáři IBM MQ” na stránce 24.
Pro ověření poskytuje produkt IBM MQ prostředek pro použití záznamů ověřování kanálu. Záznamy ověřování kanálu nabízejí přesnou kontrolu nad přístupem, který je udělen připojovacím systémům, na úrovni jednotlivých kanálů nebo skupin kanálů. Další informace viz “Záznamy ověření kanálu” na stránce 51.

Poskytování vlastního zabezpečení na úrovni odkazů
Můžete poskytnout vlastní služby zabezpečení na úrovni odkazů. Psaní vlastních kanálů výstupních programů je hlavní způsob, jak poskytnout své vlastní úroveň zabezpečení služby.

Uživatelské programy kanálu jsou zavedeny v adresáři “Uživatelské programy kanálu” na stránce 109. Stejné téma také popisuje program uživatelské procedury kanálu, který je dodáván s produktem IBM MQ for Windows (program uživatelské procedury kanálu SSPI). Tento program uživatelské procedury kanálu je dodáván ve zdrojovém formátu, takže můžete upravit zdrojový kód tak, aby vyhovoval vašim požadavkům. Pokud tento program uživatelské procedury kanálu nebo programy uživatelské procedury kanálu, které jsou k dispozici od jiných dodavatelů, nesplňují vaše požadavky, můžete navrhnout a napsat vlastní. Toto téma navrhuje způsoby, jak mohou programy uživatelských procedur kanálu poskytovat služby zabezpečení. Informace o tom, jak napsat program uživatelské procedury kanálu, naleznete v tématu Psaní programů uživatelské procedury kanálu.

Zabezpečení na úrovni propojení pomocí uživatelské procedury zabezpečení
Uživatelské procedury zabezpečení obvykle pracují ve dvojicích; jeden na každém konci kanálu. Jsou volány okamžitě po dokončení počátečního vyjednávání dat při spuštění kanálu.

Uživatelské procedury zabezpečení lze použít k identifikaci a ověření, řízení přístupu a utajení.

Zabezpečení na úrovni propojení pomocí uživatelské procedury pro zprávy
Uživatelskou proceduru zprávy lze použít pouze pro kanál zpráv, nikoli pro kanál MQI. Má přístup jak k záhlaví přenosové fronty MQXQH, které obsahuje vložený deskriptor zprávy, tak k datům aplikace ve zprávě. Může upravit obsah zprávy a změnit její délku.

Uživatelskou proceduru zprávy lze použít pro jakýkoli účel, který vyžaduje přístup k celé zprávě, a nikoli k její části.

Uživatelské procedury zpráv lze použít k identifikaci a ověření, řízení přístupu, důvěrnosti, integritě dat a neodmítání a z jiných důvodů, než je zabezpečení.

Zabezpečení na úrovni propojení pomocí uživatelských procedur pro odeslání a příjem
Uživatelské procedury pro odesílání a příjem lze použít pro kanály zpráv i MQI. Jsou volány pro všechny typy dat, která tečou kanálem, a pro toky v obou směrech.

Uživatelské procedury pro odesílání a příjem mají přístup ke každému segmentu přenosu. Mohou upravovat jeho obsah a měnit jeho délku.

Pokud v kanálu zpráv potřebuje agent MCA rozdělit zprávu a odeslat ji do více než jednoho přenosového segmentu, je pro každý přenosový segment volána uživatelská procedura pro odesílání obsahující část zprávy a na přijímacím konci je volána uživatelská procedura pro příjem pro každý přenosový segment. Totéž platí pro kanál MQI v případě, že vstupní nebo výstupní parametry volání MQI jsou příliš velké na to, aby je bylo možné odeslat v jednom přenosovém segmentu.

V kanálu MQI určuje bajt 10 přenosového segmentu volání MQI a určuje, zda přenosový segment obsahuje vstupní nebo výstupní parametry volání. Uživatelské procedury odeslání a příjmu mohou prozkoumat tento bajt a určit, zda volání MQI obsahuje data aplikace, která mohou vyžadovat ochranu.

Když je poprvé volána uživatelská procedura odeslání, aby získala a inicializovala prostředky, které potřebuje, může požádat agenta MCA, aby vyhradil určité množství prostoru ve vyrovnávací paměti, která obsahuje přenosový segment. Když je později volán ke zpracování přenosového segmentu, může tento prostor použít například k přidání šifrovaného klíče nebo digitálního podpisu. Odpovídající uživatelská procedura příjmu na druhém konci kanálu může odebrat data přidaná uživatelskou procedurou pro odesílání a použít ji ke zpracování přenosového segmentu.

Uživatelské procedury pro odesílání a příjem jsou nejvhodnější pro účely, ve kterých nepotřebují porozumět struktuře dat, s nimiž manipulují, a proto mohou s každým přenosovým segmentem zacházet jako s binárním objektem.

Uživatelské procedury pro odesílání a příjem lze použít k zajištění důvěrnosti a integrity dat a k jiným účelům, než je zabezpečení.

Související úlohy

Identifikace volání API v programu uživatelské procedury pro odeslání nebo příjem

zabezpečení na úrovni aplikace

Zabezpečení na úrovni aplikace odkazuje na služby zabezpečení, které jsou vyvolány v rozhraní mezi aplikací a správcem front, k němuž je aplikace připojena.

Tyto služby jsou vyvolány, když aplikace vydá volání MQI do správce front. Služby mohou být vyvolány přímo či nepřímo aplikací, správcem front, jiným produktem, který podporuje produkt IBM MQ, nebo kombinací těchto služeb, které spolupracují. Zabezpečení na úrovni aplikace je ilustrováno v souboru Obrázek 10 na stránce 105.

Zabezpečení na úrovni aplikace je také známé jako *komplexní zabezpečení* nebo *zabezpečení na úrovni zpráv*.

Zde je několik příkladů služeb zabezpečení na úrovni aplikací:

- Když aplikace vloží zprávu do fronty, deskriptor zprávy obsahuje ID uživatele přidružené k aplikaci. Nejsou však k dispozici žádná data, například šifrované heslo, která lze použít k ověření ID uživatele. Tato data může přidat služba zabezpečení. Když je zpráva nakonec načtena přijímající aplikací, může jiná komponenta služby ověřit ID uživatele pomocí dat, která byla se zprávou cestována. Toto je příklad identifikační a ověřovací služby.
- Zpráva může být zašifrována, když je vložena do fronty aplikací, a dešifrována, když je načtena přijímající aplikací.Toto je příklad služby důvěrnosti.
- Zprávu lze zkontrolovat, když je načtena přijímající aplikací. Tato kontrola určuje, zda byl jeho obsah od prvního vložení do fronty odesílající aplikací záměrně upraven.Toto je příklad služby integrity dat.

Plánování pro Advanced Message Security

Advanced Message Security (AMS) je komponenta produktu IBM MQ , která poskytuje vysokou úroveň ochrany citlivých dat procházejících sítí IBM MQ , aniž by to mělo vliv na koncové aplikace.

Pokud přesouváte vysoce citlivé nebo cenné informace, zejména důvěrné nebo informace související s platbou, jako jsou záznamy o pacientech nebo údaje o kreditní kartě, musíte věnovat zvláštní pozornost bezpečnosti informací. Zajištění toho, aby si informace pohybující se po celém podniku zachovala svou integritu a byla chráněna před neoprávněným přístupem, je trvalou výzvou a odpovědností. Je také pravděpodobné, že budete povinni dodržovat bezpečnostní předpisy, s rizikem sankcí za nedodržování předpisů.

Můžete vytvořit vlastní rozšíření zabezpečení produktu IBM MQ. Taková řešení však vyžadují odborné dovednosti a mohou být složitá a nákladná na údržbu. Produkt Advanced Message Security pomáhá řešit tyto problémy při přesouvání informací v rámci podniku mezi prakticky všemi typy komerčních systémů IT.

Produkt Advanced Message Security rozšiřuje funkce zabezpečení produktu IBM MQ následujícími způsoby:

- Poskytuje komplexní ochranu dat na úrovni aplikací pro infrastrukturu systému zpráv typu point-to-point s použitím šifrování nebo digitálního podepisování zpráv.
- Poskytuje komplexní zabezpečení bez nutnosti psát komplexní bezpečnostní kód nebo upravovat či znovu kompilovat existující aplikace.
- Používá technologii PKI (Public Key Infrastructure) k poskytování služeb ověřování, autorizace, důvěrnosti a integrity dat pro zprávy.
- Poskytuje správu zásad zabezpečení pro sálové počítače a distribuované servery.
- Podporuje jak servery IBM MQ , tak klienty.
- Integruje se s produktem Managed File Transfer a poskytuje komplexní řešení zabezpečeného systému zpráv.

Další informace viz "Advanced Message Security" na stránce 613.

Poskytování vlastního zabezpečení na úrovni aplikace
Můžete poskytnout vlastní služby zabezpečení na úrovni aplikace. Produkt IBM MQ poskytuje dvě uživatelské procedury, uživatelské procedury rozhraní API a uživatelské procedury pro přechod rozhraní API, které vám pomohou implementovat zabezpečení na úrovni aplikace.

Uživatelská procedura rozhraní API a uživatelská procedura přechodu rozhraní API mohou poskytovat identifikaci a ověření, řízení přístupu, důvěrnost, integritu dat a neodmítací služby a další funkce, které nesouvisejí se zabezpečením.

Pokud uživatelská procedura rozhraní API nebo uživatelská procedura přechodu rozhraní API není ve vašem systémovém prostředí podporována, možná budete chtít zvážit jiné způsoby, jak poskytnout vlastní zabezpečení na úrovni aplikace. Jedním ze způsobů je vyvinout rozhraní API vyšší úrovně, které zapouzdří rozhraní MQI. Programátoři pak místo rozhraní MQI používají toto rozhraní API k psaní aplikací IBM MQ .

Nejběžnější důvody pro použití rozhraní API vyšší úrovně jsou:

- Chcete-li skrýt rozšířené funkce rozhraní MQI před programátory.
- Chcete-li vynutit standardy při používání rozhraní MQI.
- Přidání funkce do rozhraní MQI. Touto další funkcí mohou být služby zabezpečení.

Některé dodavatelské produkty používají tuto techniku k zajištění zabezpečení na úrovni aplikace pro produkt IBM MQ.

Pokud plánujete poskytovat služby zabezpečení tímto způsobem, mějte na paměti následující informace týkající se převodu dat:

- Pokud byl token zabezpečení, například digitální podpis, přidán do dat aplikace ve zprávě, musí být jakýkoli kód provádějící převod dat informován o přítomnosti tohoto tokenu.
- Token zabezpečení mohl být odvozen z binárního obrazu dat aplikace. Proto musí být jakákoli kontrola tokenu provedena před převodem dat.
- Pokud byla data aplikace ve zprávě zašifrována, musí být před převodem dat dešifrována.

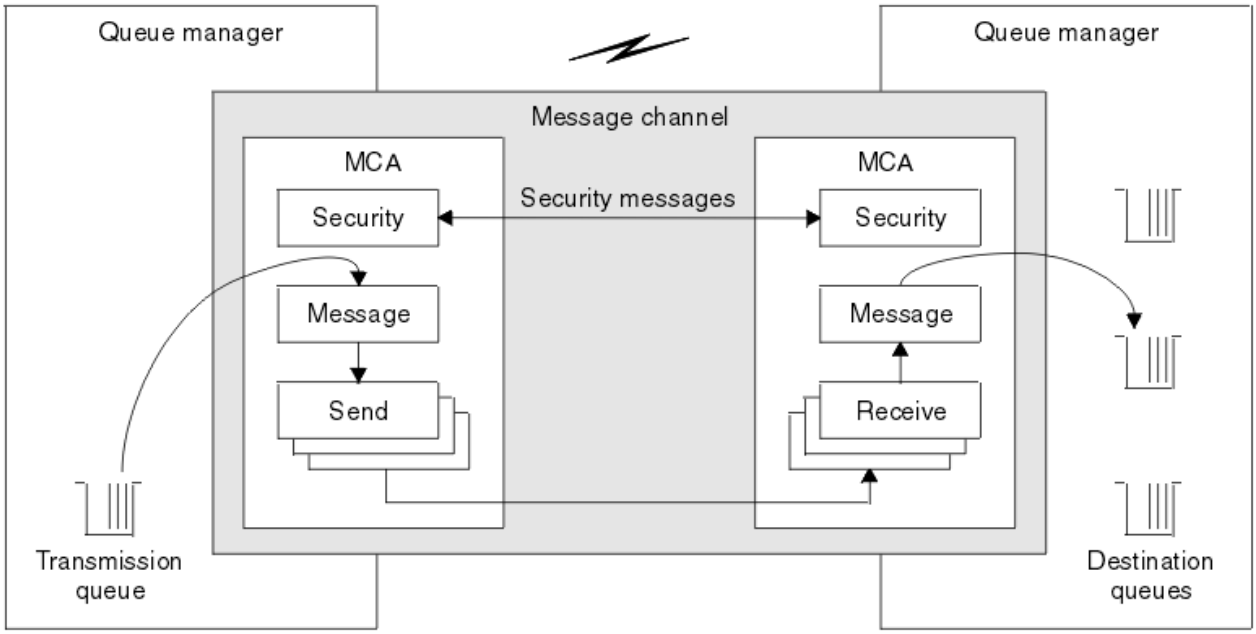
Uživatelské programy kanálu

Programy uživatelské procedury kanálu jsou programy, které jsou volány na definovaných místech v posloupnosti zpracování MCA. Uživatelé a dodavatelé mohou psát své vlastní programy výstupních kanálů. Některé jsou dodávány společností IBM.

Existuje několik typů uživatelského programu kanálu, ale pouze čtyři mají roli při poskytování zabezpečení na úrovni propojení:

- Uživatelská procedura pro zabezpečení zprávy
- Ukončení zprávy
- Ukončení odeslání
- Ukončení příjmu

Tyto čtyři typy uživatelského programu kanálu jsou ilustrovány v souboru Obrázek 11 na stránce 110 a jsou popsány v následujících tématech.



Obrázek 11. Zabezpečení, zprávy, odeslání a příjem uživatelských procedur na kanálu zpráv

Související pojmy

Programy uživatelské procedury kanálu pro kanály systému zpráv

Přehled uživatelské procedury zabezpečení

Uživatelské procedury zabezpečení obvykle pracují ve dvojicích. Jsou volány před tokem zpráv a jejich účelem je umožnit agentuře MCA ověřit svého partnera.

uživatelské procedury zabezpečení obvykle pracují ve dvojicích; jeden na každém konci kanálu. Jsou volány ihned po dokončení počátečního vyjednávání dat při spuštění kanálu, ale před tím, než začnou zprávy proudit. Primárním účelem uživatelské procedury pro zabezpečení zprávy je umožnit agentuře MCA na obou koncích kanálu ověřit svého partnera. Neexistuje však nic, co by bránilo uživatelské proceduře zabezpečení v provedení jiné funkce, dokonce ani funkce, která nemá nic společného se zabezpečením.

Uživatelské procedury zabezpečení mohou vzájemně komunikovat prostřednictvím odesílání *zpráv zabezpečení*. Formát zprávy zabezpečení není definován a je určován uživatelem. Jedním z možných výsledků výměny zpráv zabezpečení je, že jedna z uživatelských procedur zabezpečení se může rozhodnout, že nebude pokračovat dále. V takovém případě je kanál uzavřen a zprávy netečou. Pokud existuje uživatelská procedura zabezpečení pouze na jednom konci kanálu, je uživatelská procedura stále volána a může zvolit, zda má pokračovat, nebo zda má kanál zavřít.

Uživatelské procedury zabezpečení lze volat pro kanály zpráv i MQI. Název uživatelské procedury pro zabezpečení zprávy je uveden jako parametr v definici kanálu na každém konci kanálu.

Další informace o uživatelských procedur zabezpečení naleznete v tématu “Zabezpečení na úrovni propojení pomocí uživatelské procedury zabezpečení” na stránce 107.

Ukončení zprávy

Uživatelské procedury zpráv pracují pouze na kanálech zpráv a obvykle pracují ve dvojicích. Uživatelská procedura zprávy může pracovat s celou zprávou a provádět v ní různé změny.

uživatelské procedury pro zprávy na odesílajících a přijímacích koncích kanálu obvykle pracují ve dvojicích. Uživatelská procedura pro zprávy na odesílajícím konci kanálu je volána poté, co agent MCA dostal zprávu z přenosové fronty. Na přijímacím konci kanálu je před vložením zprávy MCA do cílové fronty volána uživatelská procedura pro zprávy.

Uživatelská procedura pro zprávy má přístup jak k záhlaví přenosové fronty MQXQH, které obsahuje vložený deskriptor zprávy, tak k datům aplikace ve zprávě. Uživatelská procedura zprávy může upravit obsah zprávy a změnit její délku. Změna délky může být výsledkem komprimace, dekomprimace, šifrování nebo dešifrování zprávy. Může to být také výsledkem přidání dat do zprávy nebo odebrání dat z ní.

Uživatelské procedury zpráv lze použít pro jakýkoli účel, který vyžaduje přístup k celé zprávě, spíše než k její části, a ne nutně pro zabezpečení.

Uživatelská procedura zprávy může určit, že zpráva, kterou právě zpracovává, by neměla pokračovat dále směrem k místu určení. MCA pak vloží zprávu do fronty nedoručených zpráv. Uživatelská procedura pro zprávy může také zavřít kanál.

Uživatelské procedury zpráv lze volat pouze v kanálech zpráv, nikoli v kanálech MQI. Důvodem je skutečnost, že účelem kanálu MQI je povolit vstupní a výstupní parametry volání MQI pro tok mezi aplikací IBM MQ MQI client a správcem front.

Název uživatelské procedury pro zprávy je uveden jako parametr v definici kanálu na každém konci kanálu. Můžete také určit seznam uživatelských procedur zpráv, které mají být spuštěny v posloupnosti.

Další informace o uživatelských procedur pro zprávy viz “Zabezpečení na úrovni propojení pomocí uživatelské procedury pro zprávy” na stránce 107.

Uživatelské procedury odeslání a přijetí

Uživatelské procedury odeslání a příjmu obvykle pracují ve dvojicích. Fungují na přenosových segmentech a nejlépe se používají tam, kde struktura údajů, které zpracovávají, není relevantní.

uživatelská procedura pro odesílání na jednom konci kanálu a *uživatelská procedura pro příjem* na druhém konci obvykle pracují ve dvojicích. Uživatelská procedura odeslání je volána těsně předtím, než agent MCA vydá zprávu o odeslání komunikace za účelem odeslání dat přes komunikační připojení. Uživatelská procedura pro příjem je volána bezprostředně poté, co MCA znovu získá řízení po přijetí komunikace a přijme data z komunikačního připojení. Pokud se používá sdílení konverzací přes kanál MQI, je pro každou konverzaci volána jiná instance uživatelské procedury odeslání a přijetí.

Tok protokolu kanálu IBM MQ mezi dvěma adaptéry MCA v kanálu zpráv obsahuje řídicí informace i data zpráv. Podobně v kanálu MQI obsahují toky řídicí informace a parametry volání MQI. Uživatelské procedury pro odesílání a příjem jsou volány pro všechny typy dat.

Datové toky zpráv jsou v kanálu zpráv pouze v jednom směru, v kanálu MQI však vstupní parametry toku volání MQI v jednom směru a výstupní parametry v druhém směru. V kanálech zpráv i MQI řídí informační toky v obou směrech. V důsledku toho lze uživatelské procedury pro odesílání a příjem volat na obou koncích kanálu.

Jednotka dat, která se přenáší v jednom toku mezi dvěma MCA, se nazývá *přenosový segment*. Uživatelské procedury pro odesílání a příjem mají přístup ke každému segmentu přenosu. Mohou upravovat jeho obsah a měnit jeho délku. Uživatelská procedura odeslání však nesmí měnit prvních 8 bajtů přenosového segmentu. Těchto 8 bajtů tvoří část záhlaví protokolu kanálu IBM MQ . Existují také omezení týkající se toho, kolik může uživatelská procedura odeslání zvýšit délku přenosového segmentu. Konkrétně, uživatelská procedura odeslání nemůže zvýšit svou délku nad maximum, které bylo vyjednáno mezi dvěma MCA při spuštění kanálu.

Pokud je v kanálu zpráv zpráva příliš velká na to, aby mohla být odeslána v jednom přenosovém segmentu, odesílající agent MCA zprávu rozdělí a odešle ji ve více než jednom přenosovém segmentu. V důsledku toho je volána uživatelská procedura odeslání pro každý přenosový segment obsahující část zprávy a na přijímacím konci je volána uživatelská procedura příjmu pro každý přenosový segment. Přijímající agent MCA znovu vytváří zprávu z přenosových segmentů poté, co byly zpracovány uživatelskou procedurou pro příjem.

Podobně v kanálu MQI jsou vstupní nebo výstupní parametry volání MQI odesílány ve více než jednom segmentu přenosu, pokud jsou příliš velké. K tomu může dojít například při volání MQPUT, MQPUT1nebo MQGET, pokud jsou data aplikace dostatečně velká.

Vzhledem k těmto úvahám je vhodnější používat východy pro odesílání a příjem pro účely, ve kterých nepotřebují rozumět struktuře dat, s nimiž nakládají, a mohou tedy s každým přenosovým segmentem zacházet jako s binárním objektem.

Uživatelská procedura odeslání nebo příjmu může zavřít kanál.

Názvy uživatelské procedury pro odesílání a uživatelské procedury pro příjem jsou určeny jako parametry v definici kanálu na obou koncích kanálu. Můžete také určit seznam uživatelských procedur pro odeslání, které mají být spuštěny po sobě. Podobně můžete zadat seznam uživatelských procedur pro příjem.

Další informace o uživatelských procedur pro odesílání a příjem naleznete v tématu “Zabezpečení na úrovni propojení pomocí uživatelských procedur pro odeslání a příjem” na stránce 107.

Plánování integrity dat

Naplánujte, jak zachovat integritu dat.

Integritu dat můžete implementovat na úrovni aplikace nebo na úrovni odkazu.

Na úrovni aplikace můžete použít uživatelské programy rozhraní API, pokud standardní prostředky nesplňují vaše požadavky. Můžete se rozhodnout používat produkt Advanced Message Security (AMS) k digitálnímu podepisování zpráv za účelem ochrany před neoprávněnými úpravami.

Na úrovni propojení se můžete rozhodnout používat protokol TLS. V takovém případě musíte naplánovat použití digitálních certifikátů. Můžete také použít programy výstupních kanálů, pokud standardní zařízení nesplňují vaše požadavky.

Související pojmy

“Ochrana kanálů pomocí SSL/TLS” na stránce 116
Podpora TLS v produktu IBM MQ používá objekt ověřovacích informací správce front a různé příkazy MQSC. Musíte také zvážit použití digitálních certifikátů.

“Integrita dat” na stránce 10
Služba *integrity dat* zjišťuje, zda došlo k neoprávněným úpravám dat.

“Plánování pro Advanced Message Security” na stránce 108
Advanced Message Security (AMS) je komponenta produktu IBM MQ , která poskytuje vysokou úroveň ochrany citlivých dat procházejících sítí IBM MQ , aniž by to mělo vliv na koncové aplikace.

Související odkazy

Odkaz uživatelské procedury rozhraní API

Volání uživatelské procedury kanálu a datové struktury

Plánování auditování

Rozhodněte se, která data potřebujete auditovat a jak budete zachycovat a zpracovávat informace o auditu. Zvažte, jak zkontrolovat, zda je váš systém správně nakonfigurován.

Monitorování aktivity má několik aspektů. Aspekty, které musíte zvážit, jsou často definovány požadavky auditora a tyto požadavky jsou často řízeny regulačními standardy, jako je HIPAA (Health Insurance Portability and Accountability Act) nebo SOX (Sarbanes-Oxley). Produkt IBM MQ poskytuje funkce, které mají pomoci s dodržováním těchto standardů.

Zvažte, zda máte zájem pouze o výjimky, nebo zda máte zájem o veškeré chování systému.

Některé aspekty auditování lze také považovat za provozní monitorování; jedním z rozdílů pro auditování je, že se často díváte na historická data, nikoli pouze na výstrahy v reálném čase. Monitorování je popsáno v sekci Monitorování a výkon.

Jaká data se mají auditovat

Zvažte, jaké typy dat nebo aktivity je třeba auditovat, jak je popsáno v následujících sekcích:

Změny provedené v produktu IBM MQ pomocí rozhraní IBM MQ
Nakonfigurujte produkt IBM MQ tak, aby vydával události instrumentace, konkrétně události příkazu a události konfigurace.

Změny provedené v produktu IBM MQ mimo jeho ovládací prvek
Některé změny mohou ovlivnit chování produktu IBM MQ , ale produkt IBM MQje nemůže přímo monitorovat. Příklady takových změn zahrnují změny konfiguračních souborů `mqs.ini`, `qm.ini`a `mqclient.ini`, vytvoření a odstranění správců front, instalaci binárních souborů, jako jsou uživatelské programy, a změny oprávnění k souborům. Chcete-li monitorovat tyto aktivity, musíte použít nástroje spuštěné na úrovni operačního systému. K dispozici jsou různé nástroje vhodné pro různé operační systémy. Můžete mít také protokoly vytvořené přidruženými nástroji, jako např. *sudo*.

Provozní řízení IBM MQ
Možná budete muset použít nástroje operačního systému k auditování aktivit, jako je spuštění a zastavení správců front. V některých případech lze produkt IBM MQ nakonfigurovat tak, aby vydával události instrumentace.

Aktivita aplikace v rámci IBM MQ
Chcete-li auditovat akce aplikací, například otevírání front a vkládání a získávání zpráv, nakonfigurujte produkt IBM MQ tak, aby vydával příslušné události.

Výstrahy narušitele
Chcete-li auditovat pokusy o narušení zabezpečení, nakonfigurujte systém tak, aby vydával události autorizace. Události kanálu mohou být také užitečné pro zobrazení aktivity, zejména v případě neočekávaného ukončení kanálu.

Plánování zachycení, zobrazení a archivace dat auditu

Mnoho prvků, které potřebujete, je hlášeno jako zprávy událostí IBM MQ . Musíte zvolit nástroje, které mohou číst a formátovat tyto zprávy. Máte-li zájem o dlouhodobé úložiště a analýzu, musíte je přesunout do mechanismu pomocné paměti, jako je databáze. Pokud tyto zprávy nezpracováte, zůstanou ve frontě událostí, případně frontu vyplní. Můžete se rozhodnout implementovat nástroj, který automaticky provede akci na základě některých událostí; například vydá výstrahu, když dojde k selhání zabezpečení.

Ověření, zda je váš systém správně nakonfigurován

Sada testů se dodává s produktem IBM MQ Explorer. Tyto informace použijte ke kontrole problémů s definicemi objektů.

Také pravidelně kontrolujte, zda je konfigurace systému taková, jaká očekáváte. Ačkoli mohou události příkazu a konfigurace hlásit, když se něco změní, je také užitečné vypsat konfiguraci a porovnat ji se známou dobrou kopií.

Plánování zabezpečení podle topologie

Tento oddíl se zabývá zabezpečením ve specifických situacích, konkrétně pro kanály, klastry správců front, aplikace publikování/odběru a výběrové vysílání a při použití brány firewall.

Další informace naleznete v následujících dílčích tématech:

Autorizace kanálu

Když odesíláte nebo přijímáte zprávu prostřednictvím kanálu, musíte poskytnout přístup k různým prostředkům IBM MQ . Agenti MCA (Message Channel Agent) jsou v podstatě aplikace systému IBM MQ , které přesouvají zprávy mezi správci front, a proto vyžadují přístup k různým prostředkům systému IBM MQ , aby správně fungovaly.

Chcete-li přijímat zprávy v době PUT pro MCA, můžete použít buď ID uživatele přidružené k MCA, nebo ID uživatele přidružené ke zprávě.

V době CONNECT můžete namapovat deklarovaný identifikátor uživatele na alternativního uživatele pomocí záznamů ověřování kanálu **CHLAUTH** .

V produktu IBM MQmohou být kanály chráněny podporou TLS.

ID uživatelů přidružená k odesílajícím a přijímajícím kanálům, s výjimkou odesílacího kanálu, kde není použit atribut MCAUSER, vyžadují přístup k následujícím prostředkům:

- ID uživatele přidružené k odesílajícímu kanálu vyžaduje přístup ke správci front, přenosové frontě, frontě nedoručených zpráv a přístup k dalším prostředkům vyžadovaným uživatelskými programy kanálu.
- ID uživatele MCAUSER přijímacího kanálu vyžaduje oprávnění *+ setall* . Důvodem je, že přijímací kanál musí vytvořit úplný objekt MQMD včetně všech kontextových polí s použitím dat přijatých ze vzdáleného odesílacího kanálu. Správce front proto vyžaduje, aby měl uživatel provádějící tuto aktivitu oprávnění *+ setall* . Toto oprávnění *+ setall* musí být uživateli uděleno pro:
  - Všechny fronty, do kterých přijímací kanál platně vkládá zprávy.
  - Objekt správce front. Další informace viz Oprávnění pro kontext.
- ID uživatele MCAUSER přijímacího kanálu, kde původce požadoval zprávu sestavy COA, potřebuje oprávnění *+ passid* pro přenosovou frontu, která vrací zprávu sestavy. Bez tohoto oprávnění jsou protokolovány chybové zprávy AMQ8077 .
- S ID uživatele přidruženým k přijímajícímu kanálu můžete otevřít cílové fronty a vkládat zprávy do front. Jedná se o rozhraní MQI (Message Queueing Interface), takže pokud nepoužíváte správce OAM (IBM MQ Object Authority Manager), může být nutné provést další kontroly řízení přístupu. Můžete určit, zda jsou prováděny kontroly autorizace pro ID uživatele přidružené k adaptéru MCA (jak je popsáno v tomto tématu), nebo pro ID uživatele přidružené ke zprávě (v poli MQMD UserIdentifier).

  Pro typy kanálů, na které se vztahuje, určuje parametr **PUTAUT** definice kanálu, které ID uživatele se používá pro tyto kontroly.
  - Kanál standardně používá servisní účet správce front, který má úplná administrativní oprávnění a nevyžaduje žádná speciální oprávnění.
  - V případě kanálů připojení serveru jsou administrativní připojení standardně blokována pravidly CHLAUTH a vyžadují explicitní zajišťování.
  - Kanály typu receiver, requester a cluster-receiver umožňují lokální administraci libovolným sousedním správcem front, pokud administrátor neprovede kroky k omezení tohoto přístupu.
  - Není nutné udělit oprávnění *dsp* a *ctrlx* pro ID uživatele MCAUSER přijímacího kanálu.
  - Pokud před produktem IBM MQ 8.0.0 Fix Pack 4použijete ID uživatele, které nemá oprávnění k administraci produktu IBM MQ , musíte danému ID uživatele udělit oprávnění **dsp** a **ctrlx** pro daný kanál, aby kanál fungoval.

    V systému IBM MQ 8.0.0 Fix Pack 4neexistují žádné kontroly oprávnění, když se kanál znovu synchronizuje a opravuje pořadová čísla.

    Avšak ruční zadání příkazu RESET CHANNEL stále vyžaduje **+dsp** a **+ctrlx** ve všech vydáních.

    Upozornění: Je-li pro potvrzení dávky zpráv vyžadován reset kanálu, produkt IBM MQ se pokusí o zadání dotazu na kanál, který vyžaduje oprávnění **+dsp** .
  - Atribut MCAUSER není pro typ kanálu SDR použit.
  - Pokud použijete ID uživatele přidružené ke zprávě, je pravděpodobné, že ID uživatele pochází ze vzdáleného systému. Toto ID uživatele vzdáleného systému musí být rozpoznáno cílovým systémem. Následující příkazy jsou příklady typu příkazu, který můžete zadat pro udělení oprávnění ID uživatele ze vzdáleného systému:

```
setmqaut -m QMgrName -t qmgr -g GroupName +connect +inq +setall
```

```
setmqaut -m QMgrName -t chl -n Profile -g GroupName +dsp +ctrlx
```

kde *Profil* je kanál.

```
setmqaut -m QMgrName -t q -n Profile -g GroupName +put +setall
```

kde *Profil* je fronta nedoručených zpráv, je-li nastavena.

```
setmqaut -m QMgrName -t q -n Profile -g GroupName +put +setall
```

kde *Profil* je seznam autorizovaných front.

Upozornění: Buďte opatrní při autorizaci ID uživatele pro umístění zpráv do fronty příkazů nebo jiných citlivých systémových front.

ID uživatele přidružené k adaptéru MCA závisí na typu agenta MCA. Existují dva typy MCA:

Volající MCA
MCA, které iniciují kanál. Adaptéry MCA volajícího lze spustit jako jednotlivé procesy, jako podprocesy inicializátoru kanálu nebo jako podprocesy fondu procesů. Použité ID uživatele je ID uživatele přidružené k nadřízenému procesu (iniciátoru kanálu) nebo ID uživatele přidružené k procesu, který spouští agenta MCA.

Odpovídající agent MCA
Odpovídající MCA jsou MCA, které jsou spuštěny jako výsledek požadavku volajícího MCA. Odpovídající adaptéry MCA lze spustit jako jednotlivé procesy, jako podprocesy modulu listener nebo jako podprocesy fondu procesů. ID uživatele může být jedním z následujících typů (v tomto pořadí předvoleb):

1. Na APPC může volající MCA označit ID uživatele, které se má použít pro odpovídající MCA. Toto se nazývá ID uživatele sítě a vztahuje se pouze na kanály spuštěné jako jednotlivé procesy. Nastavte ID uživatele sítě pomocí parametru USERID definice kanálu.
2. Není-li parametr **USERID** použit, může definice kanálu agenta MCA odpovídacího modulu určovat jméno uživatele, které musí agent MCA používat. Nastavte ID uživatele pomocí parametru **MCAUSER** definice kanálu.
3. Pokud ID uživatele nebylo nastaveno žádnou z předchozích (dvou) metod, použije se ID uživatele procesu, který spouští agenta MCA, nebo ID uživatele nadřízeného procesu (modulu listener).

Související pojmy

“Záznamy ověření kanálu” na stránce 51
Chcete-li zlepšit kontrolu nad udílením přístupu k připojujícím se systémům na úrovni kanálu, můžete použít záznamy ověření kanálu.

Související odkazy

Vlastnosti záznamu ověření kanálu

Ochrana definic inicializátoru kanálu

S iniciátory kanálu mohou manipulovat pouze členové skupiny mqm.

IBM MQ inicializátory kanálu nejsou IBM MQ objekty; přístup k nim není řízen modulem OAM. Produkt IBM MQ neumožňuje uživatelům nebo aplikacím manipulovat s těmito objekty, pokud jejich ID uživatele není členem skupiny mqm. Máte-li aplikaci, která zadá příkaz PCF **StartChannelInitiator**, musí být ID uživatele zadané v deskriptoru zprávy PCF členem skupiny mqm v cílovém správci front.

ID uživatele musí být také členem skupiny mqm na cílovém počítači, aby bylo možné zadat ekvivalentní příkazy MQSC prostřednictvím příkazu Escape PCF nebo pomocí příkazu `runmqsc` v nepřímém režimu.

Přenosové fronty

Správci front automaticky vkládají vzdálené zprávy do přenosové fronty; k tomu není vyžadováno žádné speciální oprávnění.

Pokud však potřebujete vložit zprávu přímo do přenosové fronty, vyžaduje to speciální oprávnění; viz Tabulka 12 na stránce 133.

Uživatelské procedury kanálu

Pokud záznamy ověřování kanálu nejsou vhodné, můžete pro zvýšení zabezpečení použít uživatelské procedury kanálu. Uživatelská procedura zabezpečení vytváří zabezpečené připojení mezi dvěma

programy uživatelské procedury zabezpečení. Jeden program je určen pro agenta MCA (odeslání kanálu zpráv) a jeden je určen pro přijímající agenta MCA.

Další informace o uživatelských procedur kanálu naleznete v části “Uživatelské programy kanálu” na stránce 109 .

Ochrana kanálů pomocí SSL/TLS

Podpora TLS v produktu IBM MQ používá objekt ověřovacích informací správce front a různé příkazy MQSC. Musíte také zvážit použití digitálních certifikátů.

Digitální certifikáty a úložiště klíčů

Je dobrým zvykem nastavit atribut popisku certifikátu správce front (**CERTLABL**). na název osobního certifikátu, který má být použit pro většinu kanálů, a přepsat jej pro výjimky nastavením popisku certifikátu na těch kanálech, které vyžadují různé certifikáty.

Potřebujete-li mnoho kanálů s certifikáty, které se liší od výchozího certifikátu nastaveného ve správci front, měli byste zvážit rozdělení kanálů mezi několik správců front nebo použít server proxy MQIPT před správcem front k předložení jiného certifikátu.

Pro každý kanál můžete použít jiný certifikát, ale pokud do úložiště klíčů uložíte příliš mnoho certifikátů, můžete očekávat, že při spouštění kanálů TLS dojde k ovlivnění výkonu. Pokuste se zachovat počet certifikátů v úložišti klíčů na méně než 50 a považujte hodnotu 100 za maximum, protože výkon systému IBM Global Security Kit (GSKit) se prudce snižuje u větších úložišť klíčů.

Povolení více certifikátů ve stejném správci front zvyšuje pravděpodobnost, že ve stejném správci front bude použito více certifikátů CA. Tím se zvýší pravděpodobnost, že obor názvů rozlišujícího názvu předmětu certifikátu bude v rozporu s certifikáty vydanými samostatnými certifikačním úřadem.

Zatímco profesionální certifikační autority jsou pravděpodobně opatrnější, interní certifikační autority často postrádají jasné konvence pojmenování a vy byste mohli skončit s nezamýšlenými shodami mezi jednou CA a druhou.

Kromě rozlišujícího názvu subjektu byste měli zkontrolovat rozlišující název vydavatele certifikátu. Chcete-li tak učinit, použijte záznam SSLPEERMAP ověření kanálu a nastavte pole **SSLPEER** a **SSLCERTI** tak, aby se shodovala s DN subjektu a DN vydavatele.

Certifikáty podepsané sebou samým a certifikáty podepsané certifikační autoritou

Je důležité naplánovat používání digitálních certifikátů, a to jak při vývoji a testování aplikace, tak i pro její použití v produkci. V závislosti na použití správců front a klientských aplikací můžete použít certifikáty podepsané certifikační autoritou nebo certifikáty podepsané držitelem.

Certifikáty podepsané certifikační autoritou
V případě produkčních systémů získejte certifikáty od důvěryhodné certifikační autority (CA). Když obdržíte certifikát od externí CA, zaplatíte za službu.

Certifikáty podepsané svým držitelem
Při vývoji aplikace můžete používat certifikáty podepsané svým držitelem nebo certifikáty vydané lokální CA, v závislosti na platformě:

ALW V systémech AIX, Linux, and Windows můžete používat certifikáty podepsané sebou samým. Pokyny naleznete v části “Vytvoření osobního certifikátu podepsaného (svým) držitelem v systému AIX, Linux, and Windows” na stránce 308.

IBM i V systémech IBM i můžete použít certifikáty podepsané lokální CA. Pokyny naleznete v části “Vyžádání certifikátu serveru v systému IBM i” na stránce 286 .

z/OS V systému z/OSmůžete použít buď certifikáty podepsané sebou samým, nebo certifikáty podepsané lokální CA. Pokyny viz “Vytvoření osobního certifikátu podepsaného (svým) držitelem v systému z/OS” na stránce 335 nebo “Vyžádání osobního certifikátu na z/OS” na stránce 335 .

Certifikáty podepsané svým držitelem nejsou vhodné pro produkční použití, a to z následujících důvodů:

- Certifikáty podepsané svým držitelem nelze odvolat, což může útočníkovi umožnit, aby po ohrožení soukromého klíče zfalšoval identitu. Certifikační autority mohou odvolat ohrožený certifikát, což brání jeho dalšímu použití. Certifikáty podepsané certifikační autoritou jsou proto bezpečnější pro použití v produkčním prostředí, ačkoli certifikáty podepsané sebou samým jsou pro testovací systém pohodlnější.
- Platnost certifikátů podepsaných svým držitelem nikdy nevyprší. To je pohodlné a bezpečné v testovacím prostředí, ale v produkčním prostředí je ponechává otevřené případným narušením zabezpečení. Riziko je spojeno se skutečností, že certifikáty podepsané sebou samým nelze odvolat.
- Certifikát podepsaný svým držitelem se používá jak jako osobní certifikát, tak jako kořenový (nebo kotva důvěryhodnosti) certifikát CA. Uživatel s osobním certifikátem podepsaným držitelem jej může používat k podepisování jiných osobních certifikátů. Obecně to neplatí pro osobní certifikáty vydané certifikační autoritou a představuje významnou expozici.

CipherSpecs a digitální certifikáty

Se všemi podporovanými typy digitálních certifikátů lze použít pouze podmnožinu podporovaných specifikací CipherSpecs . Proto je nutné zvolit vhodnou specifikaci CipherSpec pro vaše digitální certifikáty. Podobně, pokud zásada zabezpečení vaší organizace vyžaduje použití konkrétní CipherSpec , musíte získat vhodné digitální certifikáty.

Další informace o vztahu mezi specifikacemi CipherSpecs a digitálními certifikáty viz “Digitální certifikáty a kompatibilita CipherSpec v produktu IBM MQ” na stránce 46 .

Zásady ověřování certifikátů

Standard IETF RFC 5280 specifikuje řadu pravidel pro ověření platnosti certifikátu, která musí být v souladu s aplikačním softwarem implementována, aby se zabránilo útokům na zosobnění. Sada pravidel pro ověření platnosti certifikátu se nazývá zásada ověření platnosti certifikátu. Další informace o zásadách ověřování certifikátů v tématu IBM MQnaleznete v části “Zásady ověřování certifikátů v adresáři IBM MQ” na stránce 44.

Plánování kontroly odvolání certifikátů

Povolení více certifikátů od různých certifikačních autorit může způsobit zbytečnou dodatečnou kontrolu odvolání certifikátů.

Pokud jste výslovně nakonfigurovali použití serveru odvolání od konkrétní certifikační autority, například pomocí objektu AUTHINFO nebo struktury záznamu ověřovacích informací (MQAIR), kontrola odvolání selže, pokud je předložena s certifikátem od jiné certifikační autority.

Měli byste se vyvarovat explicitní konfigurace serveru odvolání certifikátů. Místo toho byste měli povolit implicitní kontrolu, kde každý certifikát obsahuje své vlastní umístění serveru odvolání v rozšíření certifikátu, například distribuční místo CRL nebo přístup OCSP AuthorityInfo.

Další informace viz OCSPCheckExtensions a CDPCheckExtensions.

Příkazy a atributy pro podporu TLS

Protokol TLS (Transport Layer Security) poskytuje zabezpečení kanálu s ochranou proti odposlechu, manipulaci a zosobnění. Podpora produktu IBM MQ pro protokol TLS umožňuje určit v definici kanálu, že konkrétní kanál používá zabezpečení TLS. Můžete také zadat podrobnosti o typu požadovaného zabezpečení, jako je například šifrovací algoritmus, který chcete použít.

- Následující příkazy MQSC podporují TLS:

  ALTER AUTHINFO
  Upraví atributy objektu ověřovacích informací.

PŘEDEFINOVÁNO AUTHINFO
Vytvoří objekt ověřovacích informací.

DELETE AUTHINFO (ODSTRANĚNÍ)
Odstraní objekt ověřovacích informací.

ZOBRAZENÍ AUTHINFO
Zobrazí atributy pro specifický objekt ověřovacích informací.

- Následující parametry správce front podporují protokol TLS:

CERTLABL
Definuje popisek osobního certifikátu, který se má použít.

V 9.3.0 V 9.3.0 **KEYRPWD**
Na systémech AIX, Linux, and Windows definuje heslo, které produkt IBM MQ používá pro přístup k úložišti klíčů. Toto pole je šifrováno pomocí systému ochrany hesla.

SSLCRLNL
Atribut SSLCRLNL uvádí seznam názvů objektů ověřovacích informací, které se používají k poskytnutí umístění odvolaných certifikátů pro povolení rozšířené kontroly certifikátů TLS.

SSLCRYP
V systémech AIX, Linux, and Windows nastaví atribut správce front **SSLCryptoHardware** . Tento atribut je název řetězce parametru, který můžete použít ke konfiguraci šifrovacího hardwaru, který máte v systému.

SSLEV
Určuje, zda je hlášena zpráva o události TLS, pokud kanál používající TLS nevytvoří připojení TLS.

SSLFIPS
Uvádí, zda se mají použít pouze algoritmy certifikované FIPS, pokud se šifrování provádí v produktu IBM MQ , spíše než v šifrovacím hardwaru. Je-li kryptografický hardware nakonfigurován, použijí se šifrovací moduly poskytované hardwarovým produktem, které mohou být certifikovány podle standardu FIPS na konkrétní úroveň. To závisí na používaném hardwarovém produktu.

SSLKEYR
V systémech AIX, Linux, and Windows přidruží úložiště klíčů ke správci front. Produkt GSKit vám umožňuje používat zabezpečení TLS na systémech AIX, Linux, and Windows .

SSLRKEYC
Počet bajtů, které se mají odeslat a přijmout v rámci konverzace TLS, než se znovu vyjedná tajný klíč. Počet bajtů zahrnuje řídicí informace odeslané MCA.

- Následující parametry kanálu podporují protokol TLS:

CERTLABL
Definuje popisek osobního certifikátu, který se má použít.

SSLCAUTH
Definuje, zda produkt IBM MQ vyžaduje a ověřuje certifikát od klienta TLS.

SSLCIPH
Uvádí sílu šifrování a funkci (CipherSpec), například TLS_RSA_WITH_AES_128_CBC_SHA. CipherSpec se musí shodovat na obou koncích kanálu.

SSLPEER
Určuje rozlišující název (jedinečný identifikátor) povolených partnerů.

Tento oddíl popisuje příkazy **setmqaut**, **dspmqaut**, **dmpmqaut**, **rcrmqobj**, **rcdmqimg**a **dspmqfls** pro podporu objektu ověřovacích informací. Také popisuje příkazy **runmqckm** (iKeycmd) a **runmqakm** pro správu certifikátů v systému AIX, Linux, and Windows. Viz následující sekce:

- setmqaut
- dspmqaut
- dmpmqaut
- rcrmqobj

- rcdmqimg
- dspmqfls
- Správa klíčů a certifikátů

Přehled zabezpečení kanálu pomocí protokolu TLS naleznete v tématu

- “Protokoly zabezpečení TLS v adresáři IBM MQ” na stránce 24

Podrobnosti o příkazech MQSC přidružených k protokolu TLS viz

- ALTER AUTHINFO
- DEFINE AUTHINFO
- DELETE AUTHINFO
- ZOBRAZIT INFORMACE O OVĚŘENÍ

Podrobnosti o příkazech PCF přidružených k protokolu TLS naleznete v tématu

- Změnit, kopírovat a vytvořit objekt ověřovacích informací
- Odstranit objekt ověřovacích informací
- Zjistit objekt ověřovacích informací

z/OS *IBM MQ for z/OS Kanál připojení serveru*

Kanál IBM MQ for z/OS SVRCONN není zabezpečený bez implementace ověřování kanálu nebo bez přidání uživatelské procedury zabezpečení pomocí protokolu TLS. Kanály VRCONN nemají standardně definovanou uživatelskou proceduru zabezpečení.

Obavy o bezpečnost

Kanály VRCONN nejsou zabezpečené, jak bylo původně definováno, SYSTEM.DEF.SVRCONN . Chcete-li zabezpečit kanál SVRCONN, musíte nastavit ověření kanálu pomocí příkazu SET CHLAUTH nebo nainstalovat uživatelskou proceduru zabezpečení a implementovat TLS.

Musíte použít veřejně dostupnou ukázkovou uživatelskou proceduru pro zabezpečení zprávy, napsat uživatelskou proceduru pro zabezpečení zprávy sami nebo zakoupit uživatelskou proceduru pro zabezpečení zprávy.

K dispozici je několik ukázek, které můžete použít jako dobrý výchozí bod pro zápis vlastní uživatelské procedury zabezpečení kanálu SVRCONN.

V systému IBM MQ for z/OSje člen CSQ4BCX3 v knihovně hlq.SCSQC37S ukázkou uživatelské procedury zabezpečení napsanou v jazyce C. Ukázka CSQ4BCX3 je také předkompilována ve vaší knihovně hlq.SCSQAUTH .

Ukázkovou uživatelskou proceduru CSQ4BCX3 můžete implementovat zkopírováním kompilovaného člena hlq.SCSQAUTH(CSQ4BCX3) do zaváděcí knihovny, která je přidělena pro CSQXLIB DD ve vašem kanálu CHIN. Všimněte si, že CHIN vyžaduje nastavení zaváděcí knihovny jako "Program Controlled".

Změňte kanál SVRCONN tak, aby nastavil CSQ4BCX3 jako uživatelskou proceduru pro zabezpečení zprávy.

Když se klient připojí pomocí tohoto kanálu SVRCONN, CSQ4BCX3 se ověří pomocí dvojice **RemoteUserIdentifier** a **RemotePassword** z MQCD nebo z IBM MQ for z/OS 9.1.4pomocí dvojice **CSPUserIdPtr** a **CSPPasswordPtr** z MQCSP. Pokud je ověření úspěšné, zkopíruje **RemoteUserIdentifier** do **MCAUserIdentifier**a změní kontext identity podprocesu.

Pro Long Term Support a Continuous Delivery před IBM MQ for z/OS 9.1.4platí, že když se klient připojí pomocí tohoto kanálu SVRCONN, CSQ4BCX3 se ověří pomocí dvojice **RemoteUserIdentifier** a **RemotePassword** z MQCD. Pokud je ověření úspěšné, zkopíruje **RemoteUserIdentifier** do **MCAUserIdentifier**a změní kontext identity podprocesu.

Pokud píšete klienta IBM MQ Java , můžete použít rozevírací okna k dotazování uživatele a nastavení MQEnvironment.userID a MQEnvironment.password. Tyto hodnoty budou předány při vytvoření připojení.

Nyní, když máte funkční uživatelskou proceduru pro zabezpečení zprávy, je zde další problém, že ID uživatele a heslo jsou přenášeny prostým textem po síti při vytvoření připojení, stejně jako obsah všech následných zpráv produktu IBM MQ . Protokol TLS můžete použít k zašifrování těchto počátečních informací o připojení a obsahu všech zpráv systému IBM MQ .

Příklad

Pro zabezpečení IBM MQ Explorer kanálu SVRCONN SYSTEM.ADMIN.SVRCONN proveďte následující kroky:

1. Zkopírujte soubor hlq.SCSQAUTH(CSQ4BCX3) do zaváděcí knihovny, která je přidělena k CSQXLIB DD v CHINIT Proc.
2. Ověřte, že zaváděcí knihovna je Programem řízená.
3. Změňte hodnotu SYSTEM ADMIN.SVRCONN tak, aby používala uživatelskou proceduru zabezpečení CSQ4BCX3.
4. V systému IBM MQ Explorerklepněte pravým tlačítkem myši na z/OS Název správce front, vyberte volbu **Podrobnosti připojení** > **Vlastnosti** > **ID uživatele** a zadejte ID uživatele z/OS .
5. Připojte se ke správci front z/OS zadáním hesla.

Další informace

Má-li být uživatelská procedura CSQ4BCX3 spuštěna v prostředí řízeném programem, musí být vše načtené do adresního prostoru CHIN načteno z knihovny řízené programem, například ze všech knihoven v knihovně STEPLIB a všech knihoven uvedených v knihovně CSQXLIB DD. Chcete-li nastavit zaváděcí knihovnu jako příkazy RACF řízené programem. V následujícím příkladu je název zaváděcí knihovny MY.TEST.LOADLIB.

```
RALTER PROGRAM * ADDMEM('MY.TEST.LOADLIB'//NOPADCHK)
SETROPTS WHEN(PROGRAM)REFRESH
```

Chcete-li změnit kanál SVRCONN tak, aby implementoval CSQ4BCX3, zadejte následující příkaz IBM MQ :

```
ALTER CHANNEL(SYSTEM ADMIN.SVRCONN) CHLTYPE(SVRCONN) SCYEXIT(CSQ4BCX3)
```

Ve výše uvedeném příkladu je použitý název kanálu SVRCONN SYSTEM ADMIN.SVRCONN.

Další informace o uživatelských procedur kanálu naleznete v části “Uživatelské programy kanálu” na stránce 109 .

Související úlohy

Zápis programů uživatelské procedury kanálu na systému z/OS

Služby zabezpečení SNA LU 6.2

Logická jednotka SNA 6.2 nabízí šifrování na úrovni relace, ověřování na úrovni relace a ověřování na úrovni konverzace.

Poznámka: Tato kolekce témat předpokládá, že máte základní znalosti architektury SNA (Systems Network Architecture). Další dokumentace uvedená v této části obsahuje stručný úvod k příslušným pojmům a terminologii. Potřebujete-li podrobnější technický úvod do architektury SNA, viz *Technický přehled architektury systémové sítě*, GC30-3073.

LU SNA 6.2 poskytuje tři služby zabezpečení:

- Šifrování na úrovni relace
- Ověření na úrovni relace
- Ověření na úrovni konverzace

Pro šifrování na úrovni relace a ověřování na úrovni relace používá SNA algoritmus *DES (Data Encryption Standard)* . Algoritmus DES je blokový šifrovací algoritmus, který používá symetrický klíč pro šifrování a dešifrování dat. Blok i klíč mají délku 8 bajtů.

Šifrování na úrovni relace
Šifrování na úrovni relace šifruje a dešifruje data relace pomocí algoritmu DES. Lze jej tedy použít k zajištění služby utajení na úrovni linky na kanálech SNA LU 6.2 .

Logické jednotky (LU) mohou poskytovat povinné (nebo požadované) šifrování dat, selektivní šifrování dat nebo žádné šifrování dat.

V *povinné šifrovací relaci*jednotka LU šifruje všechny jednotky požadavků na odchozí data a dešifruje všechny jednotky požadavků na příchozí data.

V *výběrové šifrovací relaci*jednotka LU šifruje pouze jednotky požadavků na data určené odesílajícím transakčním programem (TP). Odesílající LU signalizuje, že data jsou šifrována, nastavením indikátoru v záhlaví požadavku. Zaškrtnutím tohoto indikátoru může přijímající LU určit, které jednotky požadavků mají být dešifrovány před jejich předáním přijímajícímu TP.

V síti SNA jsou IBM MQ MCA transakční programy. MCA nepožadují šifrování pro žádná data, která odesílají. Výběrové šifrování dat tedy není volba; v relaci je možné pouze povinné šifrování dat nebo žádné šifrování dat.

Informace o implementaci povinného šifrování dat naleznete v dokumentaci k subsystému SNA. Informace o silnějších formách šifrování, které mohou být k dispozici pro použití na vaší platformě, jako je například 24bajtové šifrování Triple DES v systému z/OS, naleznete ve stejné dokumentaci.

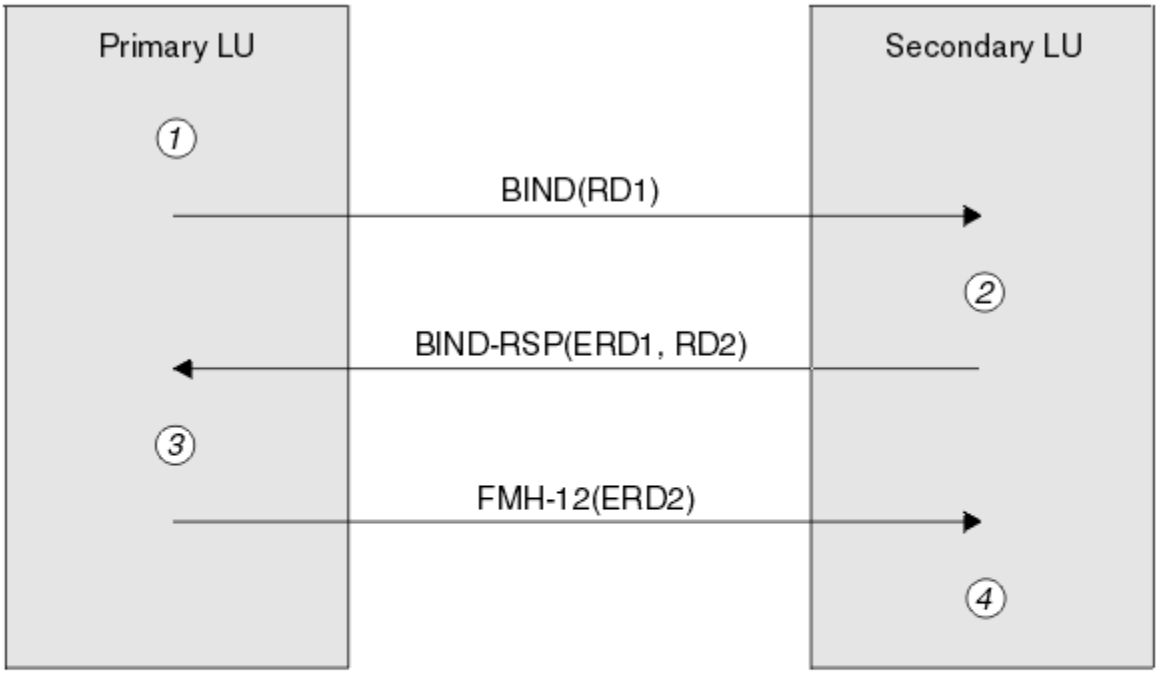
Obecnější informace o šifrování na úrovni relace viz *LU architektury systémové sítě 6.2 Odkaz: rovnocenné protokoly*, SC31-6808.

Ověření na úrovni relace
Ověřování na úrovni relace je protokol zabezpečení na úrovni relace, který umožňuje dvěma jednotkám LU vzájemné ověřování při aktivaci relace. Také se nazývá *ověřování LU-LU*.

Vzhledem k tomu, že logická jednotka je efektivně "komunikační bránou" do systému ze sítě, můžete za určitých okolností považovat tuto úroveň ověřování za dostatečnou. Pokud například váš správce front potřebuje vyměňovat zprávy se vzdáleným správcem front, který je spuštěn v řízeném a důvěryhodném prostředí, můžete být připraveni důvěřovat identitám zbývajících komponent vzdáleného systému po ověření LU.

Ověření na úrovni relace je dosaženo ověřením hesla partnera pro každou logickou jednotku. Heslo se nazývá *heslo LU-LU* , protože mezi každou dvojicí jednotek LU je zavedeno jedno heslo. Způsob vytvoření hesla LU-LU závisí na implementaci a je mimo rozsah architektury SNA.

Obrázek 12 na stránce 122 ilustruje toky pro ověření na úrovni relace.



Legend:

BIND	=	BIND request unit
BIND-RSP	=	BIND response unit
ERD	=	Encrypted random data
FMH-12	=	Function Management Header 12
RD	=	Random data

Obrázek 12. Toky pro ověření na úrovni relace

Protokol pro ověření na úrovni relace je následující. Čísla v proceduře odpovídají číslům v souboru Obrázek 12 na stránce 122.

1. Primární LU vygeneruje náhodnou datovou hodnotu (RD1) a odešle ji sekundární LU v požadavku BIND.
2. Když sekundární LU přijme požadavek BIND s náhodnými daty, zašifruje data pomocí algoritmu DES s kopií hesla LU-LU jako klíče. Sekundární LU pak vygeneruje druhou náhodnou datovou hodnotu (RD2) a odešle ji s zašifrovanými daty (ERD1) primární LU v odpovědi BIND.
3. Když primární LU obdrží odpověď BIND, vypočítá svou vlastní verzi šifrovaných dat z náhodných dat, která původně vygenerovala. Provádí to pomocí algoritmu DES s kopií hesla LU-LU jako klíče. Poté porovná svou verzi se zašifrovanými daty, která přijala v odezvě BIND. Pokud jsou obě hodnoty stejné, primární LU ví, že sekundární LU má stejné heslo jako ona a sekundární LU je ověřena. Pokud se tyto dvě hodnoty neshodují, primární LU ukončí relaci.

   Primární LU poté zašifruje náhodná data, která přijala v odezvě BIND, a odešle zašifrovaná data (ERD2) do sekundární LU v záhlaví správy funkcí 12 (FMH-12).
4. Když sekundární logická jednotka přijme FMH-12, vypočítá svou vlastní verzi šifrovaných dat z náhodně generovaných dat. Poté porovná svou verzi se zašifrovanými daty, která přijala v produktu FMH-12. Jsou-li tyto dvě hodnoty stejné, je primární LU ověřena. Pokud se tyto dvě hodnoty neshodují, sekundární LU ukončí relaci.

V rozšířené verzi protokolu, která poskytuje lepší ochranu před útoky typu man při středních útocích, sekundární logická jednotka vypočítá kód DES Message Authentication Code (MAC) z RD1, RD2a úplný název sekundární logické jednotky s použitím kopie hesla LU-LU jako klíče. Sekundární LU odešle kód MAC primární LU v odpovědi BIND namísto hodnoty ERD1.

Primární LU ověřuje sekundární LU výpočtem vlastní verze MAC, kterou porovnává s MAC přijatou v odezvě BIND. Primární LU pak vypočítá druhou MAC z RD1 a RD2a odešle MAC do sekundární LU v FMH-12 namísto ERD2.

Sekundární LU ověřuje primární LU výpočtem vlastní verze druhé MAC, kterou porovnává s MAC přijatou v FMH-12.

Informace o konfiguraci ověřování na úrovni relací naleznete v dokumentaci k subsystému SNA. Obecnější informace o ověřování na úrovni relací naleznete v tématu *LU architektury systémové sítě 6.2 Odkaz: rovnocenné protokoly*, SC31-6808.

Ověření na úrovni konverzace
Když se lokální TP pokusí přidělit konverzaci s partnerským TP, lokální LU odešle partnerské LU požadavek na připojení a požádá ji o připojení partnerského TP. Za určitých okolností může požadavek na připojení obsahovat informace o zabezpečení, které může partnerská LU použít k ověření lokálního TP. Toto se nazývá *ověření na úrovni konverzace*nebo *verifikace koncového uživatele*.

Následující témata popisují, jak produkt IBM MQ poskytuje podporu pro ověření na úrovni konverzace.

Další informace o ověřování na úrovni konverzace naleznete v tématu *LU architektury systémové sítě 6.2 Odkaz: rovnocenné protokoly*, SC31-6808.

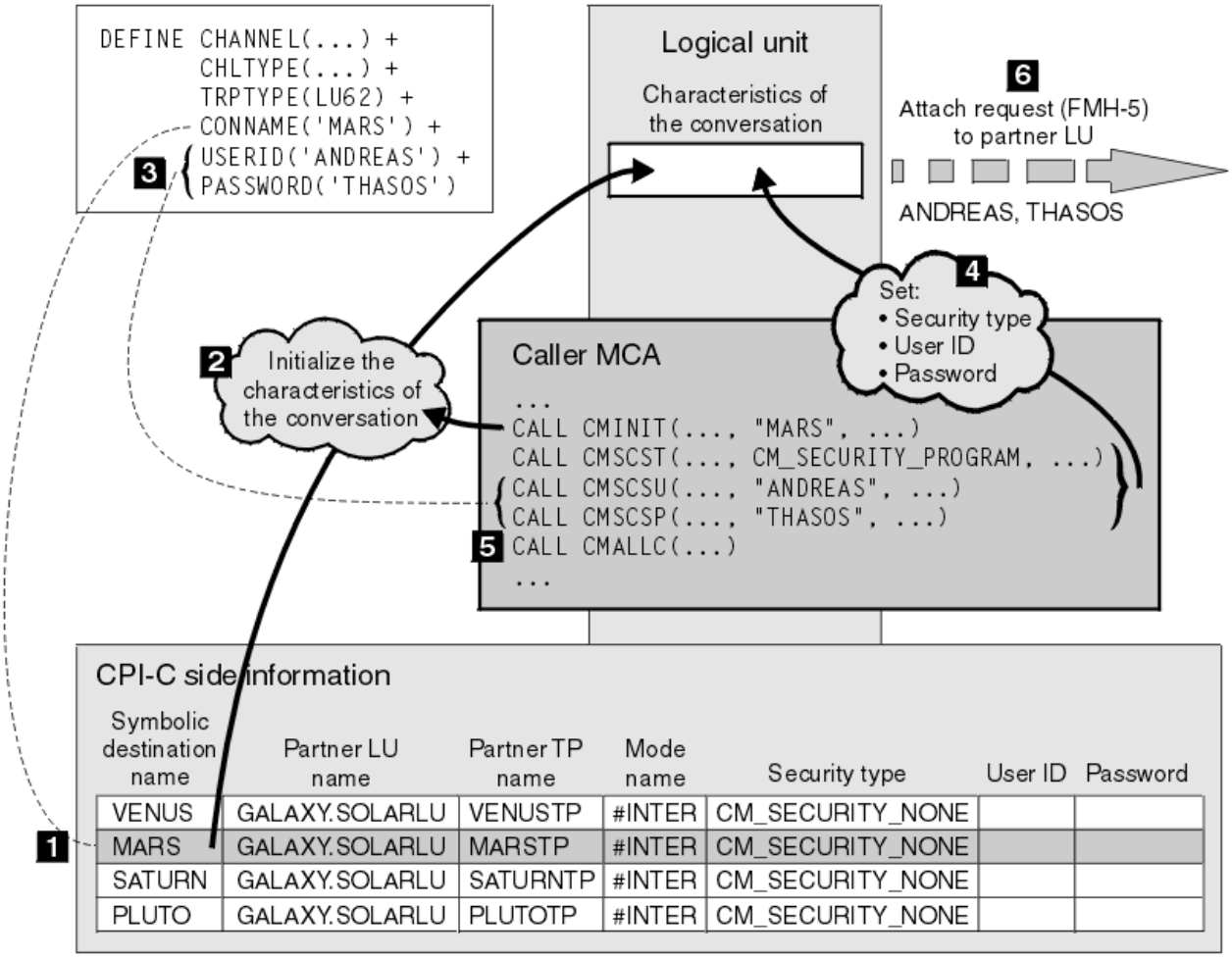
Informace specifické pro z/OSviz z/OS Plánování MVS: APPC/MVS Management.

Další informace o rozhraní CPI-C naleznete v tématu Použití komunikací CPI.

Další informace o službách APPC/MVS TP Conversation Callable Services naleznete v části Služby APPC/MVS TP Conversation Callable Services.

Multi *Podpora pro ověřování na úrovni konverzace na platformě Multiplatforms*
V tomto tématu získáte přehled o tom, jak funguje ověřování na úrovni konverzace na platformě Multiplatforms.

Podpora pro ověřování na úrovni konverzace na platformě Multiplatforms je znázorněna v tématu Obrázek 13 na stránce 124. Čísla v diagramu odpovídají číslům v následujícím popisu.



Symbolic destination name	Partner LU name	Partner TP name	Mode name	Security type	User ID	Password
VENUS	GALAXY.SOLARLU	VENUSTP	#INTER	CM_SECURITY_NONE		
MARS	GALAXY.SOLARLU	MARSTP	#INTER	CM_SECURITY_NONE		
SATURN	GALAXY.SOLARLU	SATURNTP	#INTER	CM_SECURITY_NONE		
PLUTO	GALAXY.SOLARLU	PLUTOTP	#INTER	CM_SECURITY_NONE		

Obrázek 13. Podpora IBM MQ pro ověření na úrovni konverzace

Na platformě Multiplatforms používá agent MCA volání CPI-C (Common Programming Interface Communications) ke komunikaci s partnerským agentem MCA v rámci sítě SNA. V definici kanálu na konci volajícího kanálu je hodnotou parametru CONNAME symbolický název místa určení, který identifikuje položku informací o připojení CPI-C (1). Tato položka uvádí:

- Jméno partnerské LU
- Název partnerského transakčního protokolu, který je MCA odpovídacího modulu
- Název režimu, který se má použít pro konverzaci

Položka informací o straně může také uvádět následující informace o zabezpečení:

- Typ zabezpečení.

  Běžně implementované typy zabezpečení jsou CM_SECURITY_NONE, CM_SECURITY_PROGRAM a CM_SECURITY_SAME, ale ostatní jsou definovány ve specifikaci CPI-C.
- ID uživatele.
- Heslo.

Volající agent MCA se připravuje na přidělení konverzace s respondérem MCA zadáním volání CPI-C CMINIT s použitím hodnoty CONNAME jako jednoho z parametrů volání. Volání CMINIT identifikuje ve prospěch lokální LU položku informací o straně, kterou má agent MCA v úmyslu použít pro konverzaci. Lokální LU používá hodnoty v tomto záznamu k inicializaci charakteristik konverzace (2).

Volající MCA pak zkontroluje hodnoty parametrů USERID a PASSWORD v definici kanálu (3). Je-li nastaveno USERID, volající MCA vydá následující volání CPI-C (4):

- CMSCST, chcete-li nastavit typ zabezpečení pro konverzaci na CM_SECURITY_PROGRAM.
- CMSCSU, chcete-li nastavit ID uživatele pro konverzaci na hodnotu USERID.
- CMSCSP, chcete-li nastavit heslo pro konverzaci na hodnotu PASSWORD. Není-li nastaven parametr PASSWORD, není CMSCSP volán.

Typ zabezpečení, ID uživatele a heslo nastavené těmito voláními potlačí jakékoli hodnoty získané dříve ze záznamu informací o straně.

Volající MCA pak vydá volání CPI-C CMALLC pro přidělení konverzace (5). V reakci na toto volání lokální LU odešle partnerské LU požadavek na připojení (záhlaví správy funkcí 5 nebo FMH-5) (6).

Pokud partnerská LU přijme ID uživatele a heslo, hodnoty USERID a PASSWORD se zahrnou do požadavku na připojení. Pokud partnerská LU nepřijme ID uživatele a heslo, hodnoty nejsou zahrnuty v požadavku na připojení. Lokální LU zjišťuje, zda partnerská LU přijme ID uživatele a heslo jako součást výměny informací, když se LU připojují k vytvoření relace.

V pozdější verzi požadavku na připojení může náhrada hesla proudit mezi jednotkami LU namísto čistého hesla. Náhradou hesla je ověřovací kód DES Message Authentication Code (MAC) nebo kód digest zprávy SHA-1 vytvořený z hesla. Substituci hesla lze použít pouze v případě, že je podporují obě LU.

Když partnerská LU obdrží příchozí požadavek na připojení obsahující ID uživatele a heslo, může použít ID uživatele a heslo pro účely identifikace a ověření. Na základě seznamů přístupových práv může partnerská LU také určit, zda má ID uživatele oprávnění k přidělení konverzace a připojení odpovídajícího agenta MCA.

Kromě toho může být odpovídající agent MCA spuštěn pod ID uživatele obsaženého v požadavku na připojení. V tomto případě se ID uživatele stane výchozím ID uživatele pro agenta MCA, který odpovídá, a použije se pro kontroly oprávnění, když se agent MCA pokusí připojit ke správci front. Může být také použit pro následné kontroly oprávnění, když se agent MCA pokusí o přístup k prostředkům správce front.

Způsob, jakým lze ID uživatele a heslo v požadavku na připojení použít pro identifikaci, ověření a řízení přístupu, závisí na implementaci. Informace specifické pro subsystém SNA naleznete v příslušné dokumentaci.

Není-li USERID nastaveno, volající MCA nevolá CMSCST, CMSCSU a CMSCSP. V tomto případě jsou informace o zabezpečení, které proudí v požadavku na připojení, určeny výhradně tím, co je uvedeno v položce informací o připojení a co partnerská LU přijme.

Ověření na úrovni konverzace a IBM MQ for z/OS
V tomto tématu získáte přehled o tom, jak funguje ověřování na úrovni konverzace v systému z/OS.

V systému IBM MQ for z/OSadaptéry MCA nepoužívají rozhraní CPI-C. Místo toho používají služby APPC/MVS TP Conversation Callable Services, implementaci Advanced Program-to-Program Communication (APPC), která má některé funkce CPI-C. Když volající agent MCA přidělí konverzaci, je ve volání uveden typ zabezpečení SAME. Protože logická jednotka APPC/MVS podporuje trvalé ověřování pouze pro příchozí konverzace, nikoli pro odchozí konverzace, existují dvě možnosti:

- Pokud partnerská LU důvěřuje logické jednotce APPC/MVS a přijme již ověřené ID uživatele, odešle logická jednotka APPC/MVS požadavek na připojení obsahující:
  - ID uživatele adresního prostoru inicializátoru kanálu
  - Název profilu zabezpečení, který, je-li použit parametr RACF , je názvem aktuální skupiny připojení ID uživatele adresního prostoru inicializátoru kanálu.
  - Již ověřený indikátor
- Pokud partnerská logická jednotka nedůvěřuje logické jednotce APPC/MVS a nepřijme již ověřené ID uživatele, logická jednotka APPC/MVS odešle požadavek na připojení bez informací o zabezpečení.

V systému IBM MQ for z/OSnelze parametry USERID a PASSWORD v příkazu DEFINE CHANNEL použít pro kanál zpráv a jsou platné pouze na konci připojení klienta kanálu MQI. Proto požadavek na připojení z jednotky LU APPC/MVS nikdy neobsahuje hodnoty uvedené těmito parametry.

Zabezpečení pro klastry správců front

Ačkoli použití klastrů správců front může být výhodné, je třeba věnovat zvláštní pozornost jejich zabezpečení.

Klastr správců front je síť správců front, kteří jsou nějakým způsobem logicky přidruženi. Správce front, který je členem klastru, se nazývá *správce front klastru*.

Frontu, která patří do správce front klastru, lze svěřit ostatním správcům front v klastru. Taková fronta se nazývá *fronta klastru*. Kterýkoli správce front v klastru může odesílat zprávy do front klastru bez potřeby následujících položek:

- Explicitní definice vzdálené fronty pro každou frontu klastru
- Explicitně definované kanály do a z každého vzdáleného správce front
- Samostatná přenosová fronta pro každý odchozí kanál.

Můžete vytvořit klastr, v němž jsou dva nebo více správců front klony. To znamená, že mají instance stejných lokálních front, včetně všech lokálních front deklarovaných jako fronty klastru, a mohou podporovat instance stejných serverových aplikací.

Když aplikace připojená ke správci front klastru odešle zprávu do fronty klastru, která má instanci v každém z klonovaných správců front, produkt IBM MQ rozhodne, kterému správci front ji odeslat. Když mnoho aplikací odesílá zprávy do fronty klastru, produkt IBM MQ vyrovnává pracovní zátěž mezi jednotlivými správci front, kteří mají instanci fronty. Pokud jeden ze systémů, které jsou hostiteli klonovaného správce front, selže, produkt IBM MQ pokračuje v vyrovnávání pracovní zátěže v rámci zbývajících správců front, dokud nebude systém, který selhal, restartován.

Používáte-li klastry správců front, musíte zvážit následující problémy se zabezpečením:

- Povolení odesílání zpráv správci front pouze vybraným správcům front
- Povolení odesílání zpráv do fronty ve vašem správci front pouze vybraným uživatelům vzdáleného správce front
- Povolení aplikacím připojeným ke správci front odesílat zprávy pouze do vybraných vzdálených front

Tyto aspekty jsou relevantní, i když nepoužíváte klastry, ale stávají se důležitějšími, pokud používáte klastry.

Pokud může aplikace odesílat zprávy do jedné fronty klastru, může odesílat zprávy do jiné fronty klastru, aniž by potřebovala další definice vzdálených front, přenosové fronty nebo kanály. Proto je důležitější zvážit, zda je třeba omezit přístup k frontám klastru ve správci front a omezit fronty klastru, do kterých mohou aplikace odesílat zprávy.

Existují některé další aspekty zabezpečení, které jsou relevantní pouze v případě, že používáte klastry správců front:

- Povolení připojení ke klastru pouze vybraným správcům front
- Vynucení opuštění klastru nežádoucími správci front

Další informace o všech těchto aspektech naleznete v tématu Udržování zabezpečených klastrů.

z/OS Pokyny specifické pro produkt IBM MQ for z/OSnaleznete v části “Zabezpečení v klastrech správců front v systému z/OS” na stránce 264.

Související úlohy

“Zabránění správcům front v přijímání zpráv” na stránce 499
Správci front klastru můžete zabránit v přijímání zpráv, které nemá oprávnění přijímat, pomocí uživatelských programů.

Zabezpečení pro publikování/odběr IBM MQ

Pokud používáte produkt IBM MQ Publikovat/Odebírat, existují další aspekty zabezpečení.

V systému publikování/odběru existují dva typy aplikací: vydavatel a odběratel. *Vydavatelé* poskytují informace ve formě zpráv IBM MQ . Když vydavatel publikuje zprávu, uvádí *téma*, které identifikuje předmět informací uvnitř zprávy.

Odběratelé jsou odběratelé informací, které jsou publikovány. Odběratel určuje témata, která jej zajímají, jejich přihlášením k odběru.

Správce front je aplikace dodávaná s produktem IBM MQ Publikovat/Odebírat. Přijímá publikované zprávy od vydavatelů a požadavky na odběr od odběratelů a směruje publikované zprávy k odběratelům. Odběrateli jsou odesílány zprávy pouze v těch tématech, k jejichž odběru se přihlásil.

Další informace naleznete v tématu Zabezpečení publikování/odběru.

Zabezpečení výběrového vysílání

Pomocí těchto informací můžete pochopit, proč mohou být procesy zabezpečení s výběrové vysílání produktu IBM MQ potřebné.

IBM MQ Výběrové vysílání nemá vestavěné zabezpečení. Kontroly zabezpečení jsou zpracovány ve správci front v čase MQOPEN a nastavení pole MQMD je zpracováno klientem. Některé aplikace v síti nemusí být aplikacemi IBM MQ (například aplikace LLM, viz téma Interoperabilita výběrového vysílání s IBM MQ systémem zpráv s nízkou latencí , kde získáte další informace), proto možná budete muset implementovat vlastní procedury zabezpečení, protože přijímající aplikace si nemohou být jisti platností kontextových polí.

Existují tři procesy zabezpečení, které je třeba zvážit:

Řízení přístupu

Řízení přístupu v produktu IBM MQ je založeno na ID uživatelů. Další informace o tomto tématu viz “Řízení přístupu pro klienty” na stránce 102.

Zabezpečení sítě

Izolovaná síť může být schůdnou volbou zabezpečení, která zabrání falešným zprávám. Je možné, aby aplikace na adrese skupiny výběrového vysílání publikovala škodlivé zprávy pomocí nativních komunikačních funkcí, které jsou k nerozeznání od zpráv produktu MQ , protože pocházejí z aplikace na stejné adrese skupiny výběrového vysílání.

Je také možné, aby klient na adrese skupiny výběrového vysílání přijímal zprávy, které byly určeny pro ostatní klienty na stejné adrese skupiny výběrového vysílání.

Izolováním sítě výběrového vysílání zajistíte, že přístup budou mít pouze platní klienti a aplikace. Tato bezpečnostní opatření mohou zabránit příchodu škodlivých zpráv a důvěrným informacím.

Informace o síťových adresách skupin výběrového vysílání naleznete v tématu Nastavení příslušné sítě pro přenos výběrového vysílání .

Digitální podpisy

Digitální podpis je tvořen šifrováním reprezentace zprávy. Šifrování používá soukromý klíč signatáře a z důvodu efektivity obvykle pracuje na kódu digest zprávy, nikoli na zprávě samotné. Digitální podepsání zprávy před operací MQPUT je dobrým bezpečnostním opatřením, ale tento proces může mít nepříznivý vliv na výkon, pokud existuje velký objem zpráv.

Digitální podpisy se liší podle podepsaných dat. Pokud jsou dvě různé zprávy digitálně podepsány stejnou entitou, oba podpisy se liší, ale oba podpisy lze ověřit pomocí stejného veřejného klíče, tj. veřejného klíče entity, která podepsala zprávy.

Jak již bylo zmíněno v této části, může být možné, aby aplikace na adrese skupiny výběrového vysílání publikovala škodlivé zprávy pomocí nativních komunikačních funkcí, které jsou k nerozeznání od zpráv produktu MQ . Digitální podpisy poskytují doklad o původu a pouze odesílatel zná soukromý klíč, který poskytuje přesvědčivé důkazy o tom, že odesílatel je původcem zprávy.

Další informace o tomto tématu viz “Kryptografické koncepty” na stránce 10.

Brány firewall a průchod internetem

Normálně byste použili bránu firewall, abyste zabránili přístupu z nepřátelských adres IP, například při útoku typu Denial of Service. Může však být nutné dočasně blokovat adresy IP v rámci produktu IBM MQ, například při čekání na aktualizaci pravidel brány firewall administrátorem zabezpečení.

Chcete-li blokovat jednu nebo více adres IP, vytvořte záznam ověřování kanálu typu BLOCKADDR nebo ADDRESSMAP. Další informace viz "Blokování specifických adres IP" na stránce 403.

Zabezpečení pro IBM MQ Internet Pass-Thru

Produkt IBM MQ Internet Pass-Thru může zjednodušit komunikaci prostřednictvím brány firewall, ale to má dopady na zabezpečení.

IBM MQ Internet Pass-Thru (MQIPT) je volitelná komponenta produktu IBM MQ , kterou lze použít k implementaci řešení systému zpráv mezi vzdálenými servery v Internetu.

Produkt MQIPT umožňuje dvěma správcům front výměnu zpráv nebo aplikaci klienta IBM MQ připojit se ke správci front prostřednictvím Internetu bez nutnosti přímého připojení TCP/IP. To je užitečné v případě, že brána firewall zakazuje přímé připojení TCP/IP mezi dvěma systémy. Usnadňuje průchod toků protokolů kanálu IBM MQ do brány firewall a z ní a usnadňuje jejich správu prostřednictvím tunelového propojení toků uvnitř protokolu HTTP nebo prostřednictvím funkce serveru proxy. Pomocí TLS (Transport Layer Security) lze také šifrovat a dešifrovat zprávy odesílané přes Internet.

Pokud váš systém IBM MQ komunikuje s produktem MQIPTa pokud nepoužíváte režim serveru proxy SSL v produktu MQIPT, ujistěte se, že CipherSpec používaná produktem IBM MQ odpovídá CipherSuite používané produktem MQIPT:

- Pokud produkt MQIPT vystupuje jako server TLS a produkt IBM MQ se připojuje jako klient TLS, CipherSpec použitá produktem IBM MQ musí odpovídat CipherSuite , která je povolena v příslušném svazku klíčů MQIPT .
- Pokud produkt MQIPT vystupuje jako klient TLS a připojuje se k serveru IBM MQ TLS, musí sada MQIPT CipherSuite odpovídat CipherSpec definované v přijímajícím kanálu IBM MQ .

Pokud migrujete z produktu MQIPT na integrovanou podporu TLS produktu IBM MQ , přeneste digitální certifikáty ze svazku klíčů MQIPT buď pomocí **mqiptKeyman** , nebo pomocí **mqiptKeycmd**.

Další informace viz IBM MQ Internet Pass-Thru.

z/OS IBM MQ for z/OS kontrolní seznam implementace zabezpečení

V tomto tématu je uveden podrobný postup, pomocí kterého můžete vypracovat a definovat implementaci zabezpečení pro jednotlivé správce front produktu IBM MQ .

RACF poskytuje definice pro třídy zabezpečení IBM MQ v dodané statické tabulce deskriptoru tříd (CDT). Při práci s kontrolním seznamem můžete určit, které z těchto tříd vaše nastavení vyžaduje. Musíte se ujistit, že jsou aktivovány, jak je popsáno v tématu "Třídy zabezpečení RACF" na stránce 186.

Podrobnosti viz další sekce, zejména "Profily používané k řízení přístupu k prostředkům IBM MQ" na stránce 196.

Pokud požadujete kontrolu zabezpečení, postupujte podle tohoto kontrolního seznamu, abyste jej implementovali:

1. Aktivujte třídu RACF MQADMIN (profily s velkými písmeny) nebo MXADMIN (profily se smíšenými písmeny).
   - Chcete zabezpečení na úrovni skupiny sdílení front, na úrovni správce front nebo na kombinaci obojího?

     Viz "Profily pro řízení skupiny sdílení front nebo zabezpečení na úrovni správce front" na stránce 191.
2. Potřebujete zabezpečení připojení?

- **Ano**: Aktivujte třídu MQCONN. Definujte příslušné profily připojení na úrovni správce front nebo na úrovni skupiny sdílení front ve třídě MQCONN. Poté povolte příslušným uživatelům nebo skupinám přístup k těmto profilům.

  Poznámka: Pouze uživatelé požadavku rozhraní API MQCONN nebo ID uživatelů CICS nebo IMS adresního prostoru musí mít přístup k odpovídajícímu profilu připojení.
- **Ne**: Definujte hodnotu hlq.NO.CONNECT.CHECKS na úrovni správce front nebo na úrovni skupiny sdílení front ve třídě MQADMIN nebo MXADMIN.

3. Potřebujete kontrolu zabezpečení příkazů?
   - **Ano**: Aktivujte třídu MQCMDS. Definujte příslušné profily příkazů na úrovni správce front nebo na úrovni skupiny sdílení front ve třídě MQCMDS. Poté povolte příslušným uživatelům nebo skupinám přístup k těmto profilům.

     Používáte-li skupinu sdílení front, může být nutné zahrnout jména uživatelů používaná samotným správcem front a inicializátorem kanálu. Viz “Nastavení zabezpečení prostředků IBM MQ for z/OS” na stránce 255.
   - **Ne**: Definujte hodnotu hlq.NO.CMD.CHECKS pro požadovaného správce front nebo skupinu sdílení front ve třídě MQADMIN nebo MXADMIN.
4. Potřebujete zabezpečení prostředků používaných v příkazech?
   - **Ano**: Ujistěte se, že třída MQADMIN nebo MXADMIN je aktivní. Definujte odpovídající profily pro ochranu prostředků v příkazech na úrovni správce front nebo na úrovni skupiny sdílení front ve třídě MQADMIN nebo MXADMIN. Poté povolte příslušným uživatelům nebo skupinám přístup k těmto profilům. Nastavte parametr CMDUSER v CSQ6SYSP na výchozí ID uživatele, které se má použít pro kontroly zabezpečení příkazu.

     Používáte-li skupinu sdílení front, může být nutné zahrnout jména uživatelů používaná samotným správcem front a inicializátorem kanálu. Viz “Nastavení zabezpečení prostředků IBM MQ for z/OS” na stránce 255.
   - **Ne**: Definujte hodnotu hlq.NO.CMD.RESC.CHECKS pro požadovaného správce front nebo skupinu sdílení front ve třídě MQADMIN nebo MXADMIN.
5. Potřebujete zabezpečení fronty?
   - **Ano**: Aktivujte třídu MQQUEUE nebo MXQUEUE. Definujte odpovídající profily front pro požadovaného správce front nebo skupinu sdílení front v MQQUEUE nebo MXQUEUEclass. Poté povolte příslušným uživatelům nebo skupinám přístup k těmto profilům.
   - **Ne**: Definujte hodnotu hlq.NO.QUEUE.CHECKS pro požadovaného správce front nebo skupinu sdílení front ve třídě MQADMIN nebo MXADMIN.
6. Potřebujete procesní zabezpečení?
   - **Ano**: Aktivujte třídu MQPROC nebo MXPROC. Definujte příslušné profily procesů na úrovni správce front nebo skupiny sdílení front a povolte příslušným uživatelům nebo skupinám přístup k těmto profilům.
   - **Ne**: Definujte hodnotu hlq.NO.PROCESS.CHECKS pro příslušného správce front nebo skupinu sdílení front ve třídě MQADMIN nebo MXADMIN.
7. Potřebujete zabezpečení seznamu názvů?
   - **Ano**: Aktivujte třídu MQNLIST nebo MXNLISTclass. Definujte příslušné profily seznamu názvů na úrovni správce front nebo na úrovni skupiny sdílení front ve třídě MQNLIST nebo MXNLIST. Poté povolte příslušným uživatelům nebo skupinám přístup k těmto profilům.
   - **Ne**: Definujte hodnotu hlq.NO.NLIST.CHECKS pro požadovaného správce front nebo skupinu sdílení front ve třídě MQADMIN nebo MXADMIN.
8. Potřebujete zabezpečení témat?
   - **Ano**: Aktivujte třídu MXTOPIC. Definujte odpovídající profily témat na úrovni správce front nebo na úrovni skupiny sdílení front ve třídě MXTOPIC. Poté povolte příslušným uživatelům nebo skupinám přístup k těmto profilům.

- **Ne**: Definujte hodnotu hlq.NO.TOPIC.CHECKS pro požadovaného správce front nebo skupinu sdílení front ve třídě MQADMIN nebo MXADMIN.

9. Potřebují někteří uživatelé chránit použití voleb MQOPEN nebo MQPUT1 souvisejících s použitím kontextu?
   - **Ano**: Ujistěte se, že třída MQADMIN nebo MXADMIN je aktivní. Definujte profily hlq.CONTEXT.queuename na úrovni fronty, správce front nebo skupiny sdílení front ve třídě MQADMIN nebo MXADMIN. Poté povolte příslušným uživatelům nebo skupinám přístup k těmto profilům.
   - **Ne**: Definujte hodnotu hlq.NO.CONTEXT.CHECKS pro požadovaného správce front nebo skupinu sdílení front ve třídě MQADMIN nebo MXADMIN.
10. Potřebujete chránit používání alternativních ID uživatelů?
    - **Ano**: Ujistěte se, že třída MQADMIN nebo MXADMIN je aktivní. Definujte odpovídající hlq.ALTERNATE.USER. Profily produktu *alternateuserid* pro požadovaného správce front nebo skupinu sdílení front a povolení přístupu požadovaných uživatelů nebo skupin k těmto profilům.
    - **Ne**: Definujte profil hlq.NO.ALTERNATE.USER.CHECKS pro požadovaného správce front nebo skupinu sdílení front ve třídě MQADMIN nebo MXADMIN.
11. Potřebujete upravit, která ID uživatelů se mají použít pro kontroly zabezpečení prostředků prostřednictvím RESLEVEL?
    - **Ano**: Ujistěte se, že třída MQADMIN nebo MXADMIN je aktivní. Definujte profil hlq.RESLEVEL na úrovni správce front nebo na úrovni skupiny sdílení front ve třídě MQADMIN nebo MXADMIN. Poté povolte požadované uživatele nebo skupiny pro přístup k profilu.
    - **Ne**: Ujistěte se, že ve třídě MQADMIN nebo MXADMIN neexistují žádné generické profily, které by se mohly použít pro hlq.RESLEVEL. Definujte profil hlq.RESLEVEL pro požadovaného správce front nebo skupinu sdílení front a ujistěte se, že k němu nemají přístup žádní uživatelé ani skupiny.
12. Potřebujete 'timeout' nepoužívaná ID uživatelů z IBM MQ ?
    - **Ano**: Určete, jaké hodnoty časového limitu chcete použít, a zadejte příkaz MQSC ALTER SECURITY pro změnu parametrů TIMEOUT a INTERVAL.
    - **Ne**: Zadejte příkaz MQSC ALTER SECURITY a nastavte hodnotu INTERVAL na nulu.

    Poznámka: Aktualizujte vstupní datovou sadu inicializace CSQINP1 používanou vaším subsystémem tak, aby se příkaz MQSC ALTER SECURITY zadal automaticky při spuštění správce front.
13. Používáte distribuované řazení do front?
    - **Ano**: Použít záznamy ověření kanálu. Další informace viz téma "Záznamy ověření kanálu" na stránce 51.
    - Můžete také určit odpovídající hodnotu atributu MCAUSER pro každý kanál nebo poskytnout vhodné uživatelské procedury zabezpečení kanálu.
14. Chcete použít protokol TLS (Transport Layer Security)?
    - **Ano**: Chcete-li určit, aby každý uživatel, který předkládá osobní certifikát TLS obsahující uvedené DN, používal určitého uživatele MCAUSER, nastavte záznam ověřování kanálu typu SSLPEERMAP. Můžete zadat jeden rozlišující název nebo vzorec zahrnující zástupné znaky.
    - Naplánujte si svou infrastrukturu TLS. Nainstalujte funkci System SSL produktu z/OS. V produktu RACFnastavte filtry názvů certifikátů (CNF), pokud je používáte, a digitální certifikáty. Nastavte svazek klíčů SSL. Ujistěte se, že atribut správce front SSLKEYR není prázdný a ukazuje na svazek klíčů SSL. Také se ujistěte, že hodnota SSLTASKS je alespoň 2.
    - **Ne**: Ujistěte se, že SSLKEYR je prázdné a SSLTASKS je nula.

    Další podrobnosti o protokolu TLS viz "Protokoly zabezpečení TLS v adresáři IBM MQ" na stránce 24.
15. Používáte klienty?
    - **Ano**: Použít záznamy ověření kanálu.

- Můžete také určit odpovídající hodnotu atributu MCAUSER pro každý kanál připojení serveru nebo v případě potřeby poskytnout vhodné uživatelské procedury zabezpečení kanálu.

16. Zkontrolujte nastavení přepínače.

    Produkt IBM MQ vydává zprávy při spuštění správce front, který zobrazuje vaše nastavení zabezpečení. Pomocí těchto zpráv určete, zda jsou přepínače správně nastaveny.

17. Posíláte hesla z klientských aplikací?

    - **Ano**: Ujistěte se, že je nainstalována funkce z/OS a že je spuštěn ICSF (Integrated Cryptographic Service Facility) pro nejlepší ochranu.
    - **Ne**: Můžete ignorovat hlášení o chybových zprávách, že nebylo spuštěno ICSF.

    Další informace o ICSF viz “Použití ICSF (Integrated Cryptographic Service Facility)” na stránce 264

Nastavení zabezpečení

Tato kolekce témat obsahuje informace specifické pro různé operační systémy a pro použití klientů.

ALW Nastavení zabezpečení na systému AIX, Linux, and Windows

Aspekty zabezpečení specifické pro systémy AIX, Linux, and Windows .

Správci front IBM MQ přenášejí informace, které jsou potenciálně cenné, takže je třeba použít systém oprávnění, abyste zajistili, že neautorizovaní uživatelé nebudou mít přístup k vašim správcům front. Zvažte následující typy ovládacích prvků zabezpečení:

Kdo může spravovat IBM MQ
Můžete definovat sadu uživatelů, kteří mohou vydávat příkazy pro správu produktu IBM MQ.

Kdo může používat objekty IBM MQ
Můžete definovat, kteří uživatelé (obvykle aplikace) mohou používat volání MQI a příkazy PCF k provedení následujících akcí:

- Kdo se může připojit ke správci front.
- Kdo může přistupovat k objektům (frontám, definicím procesů, seznamům názvů, kanálům, kanálům připojení klienta, modulům listener, službám a objektům ověřovacích informací) a jaký typ přístupu k těmto objektům mají.
- Kdo má přístup ke zprávám IBM MQ .
- Kdo má přístup k informacím o kontextu přidruženým ke zprávě.

Zabezpečení kanálu
Je třeba zajistit, aby kanály používané k odesílání zpráv na vzdálené systémy měly přístup k požadovaným prostředkům.

K udělení přístupu ke knihovnám programů, knihovnám odkazů MQI a příkazům můžete použít standardní provozní prostředky. Avšak adresář obsahující fronty a další data správce front je pro produkt IBM MQsoukromý; nepoužívejte standardní příkazy operačního systému k udělení nebo zrušení oprávnění pro prostředky MQI.

ALW Jak fungují autorizace na produktu AIX, Linux, and Windows

Tabulky specifikace autorizace v tématech v této sekci přesně definují, jak autorizace fungují a jaká omezení platí.

Tabulky platí pro tyto situace:

- Aplikace, které volají rozhraní MQI
- Administrační programy, které vydávají příkazy MQSC jako řídicí PCF
- Administrační programy, které vydávají příkazy PCF

V této sekci jsou informace prezentovány jako sada tabulek, které určují následující:

Akce, která se má provést
Volba MQI, příkaz MQSC nebo příkaz PCF.

Objekt řízení přístupu
Fronta, proces, správce front, seznam názvů, ověřovací informace, kanál, kanál připojení klienta, modul listener nebo služba.

Je vyžadována autorizace
Vyjádřeno jako konstanta MQZAO_.

V tabulkách konstanty s předponou MQZAO_ odpovídají klíčovým slovům v seznamu oprávnění pro příkaz `setmqaut` pro konkrétní entitu. Například MQZAO_BROWSE odpovídá klíčovému slovu `+browse`, MQZAO_SET_ALL_CONTEXT odpovídá klíčovému slovu `+setallatd`. Tyto konstanty jsou definovány v hlavičkovém souboru cmqzc.hdodávaném s produktem.

ALW *Autorizace pro volání MQI*

MQCONN, **MQOPEN**, **MQPUT1**a **MQCLOSE** mohou vyžadovat kontroly autorizace. Tabulky v tomto tématu shrnují autorizace potřebné pro každé volání.

Aplikace může vydávat specifická volání a volby MQI pouze v případě, že identifikátoru uživatele, pod kterým je spuštěna (nebo jehož autorizací lze předpokládat), byla udělena příslušná autorizace.

Čtyři volání MQI mohou vyžadovat kontroly autorizace: **MQCONN**, **MQOPEN**, **MQPUT1**a **MQCLOSE**.

Pro **MQOPEN** a **MQPUT1**se provede kontrola oprávnění na názvu otevíraného objektu, a ne na názvu nebo názvech, což bude mít za následek vyřešení názvu. Aplikaci může být například uděleno oprávnění k otevření alias fronty, aniž by měla oprávnění k otevření základní fronty, pro kterou je alias vyhodnocován. Pravidlem je, že kontrola se provádí u první definice zjištěné během procesu interpretace názvu, který není aliasem správce front, pokud není definice aliasu správce front otevřena přímo; to znamená, že její název se zobrazí v poli *ObjectName* deskriptoru objektu. Oprávnění je vždy potřebné pro otevíraný objekt. V některých případech je vyžadováno další oprávnění nezávislé na frontě získané prostřednictvím autorizace pro objekt správce front.

Tabulka 10 na stránce 132, Tabulka 11 na stránce 132, Tabulka 12 na stránce 133a Tabulka 13 na stránce 134 shrnují autorizace potřebné pro každé volání. V tabulkách *Nelze použít* znamená, že kontrola autorizace není pro tuto operaci relevantní. *Žádná kontrola* znamená, že se neprovádí žádná kontrola autorizace.

Poznámka: V těchto tabulkách nenajdete žádnou zmínku o seznamech názvů, kanálech, kanálech připojení klienta, modulech listener, službách nebo objektech ověřovacích informací. Důvodem je, že na tyto objekty se nevztahuje žádná z autorizací, s výjimkou oprávnění MQOO_INQUIRE, pro která platí stejná autorizace jako pro ostatní objekty.

Speciální autorizace MQZAO_ALL_MQI zahrnuje všechny autorizace v tabulkách, které jsou relevantní pro daný typ objektu, s výjimkou MQZAO_DELETE a MQZAO_DISPLAY, které jsou klasifikovány jako administrativní autorizace.

Chcete-li upravit kteroukoli z voleb kontextu zprávy, musíte mít příslušná oprávnění k vydání volání. Chcete-li například použít MQOOO_SET_IDENTITY_CONTEXT nebo MQPMO_SET_IDENTITY_CONTEXT, musíte mít oprávnění `+setid` .

Tabulka 10. Bezpečnostní autorizace potřebná pro volání MQCONN

Autorizace vyžadovaná pro:	Objekt fronty (“1” na stránce 134)	Objekt procesu	Objekt správce front
MQCONN	Nelze použít	Nelze použít	MQZAO_CONNECT

Tabulka 11. Bezpečnostní autorizace potřebná pro volání MQOPEN

Autorizace vyžadovaná pro:	Objekt fronty (“1” na stránce 134)	Objekt procesu	Objekt správce front
MQOO_DOTAZOVAT	MQZAO_INQUIRE	MQZAO_INQUIRE	MQZAO_INQUIRE

Tabulka 11. Bezpečnostní autorizace potřebná pro volání MQOPEN (pokračování)			
Autorizace vyžadovaná pro:	**Objekt fronty ("1" na stránce 134)**	**Objekt procesu**	**Objekt správce front**
MQOO_BROWSE	MQZAO_BROWSE	Nelze použít	Bez kontroly
MQOO_INPUT_ *	MQZAO_INPUT	Nelze použít	Bez kontroly
MQOO_SAVE_ ALL_CONTEXT **("2" na stránce 134)**	MQZAO_INPUT	Nelze použít	Nelze použít
MQOO_OUTPUT (normální fronta) **("3" na stránce 134)**	MQZAO_OUTPUT	Nelze použít	Nelze použít
MQOO_PASS_ IDENTITY_CONTEXT **("4" na stránce 134)**	MQZAO_PASS_ IDENTITY_CONTEXT	Nelze použít	Bez kontroly
KONTEXT MQOO_PASS_ALL_ **("4" na stránce 134, "5" na stránce 134)**	MQZAO_PASS _ALL_CONTEXT	Nelze použít	Bez kontroly
MQOO_SET_ IDENTITY_CONTEXT **("4" na stránce 134, "5" na stránce 134)**	MQZAO_SET_ IDENTITY_CONTEXT	Nelze použít	MQZAO_SET_ IDENTITY_CONTEXT **("6" na stránce 134)**
MQOO_SET_ ALL_CONTEXT **("4" na stránce 134, "7" na stránce 134)**	MQZAO_SET_ ALL_CONTEXT	Nelze použít	MQZAO_SET_ ALL_CONTEXT **("6" na stránce 134)**
MQOO_OUTPUT (přenosová fronta) **("8" na stránce 134)**	MQZAO_SET_ ALL_CONTEXT	Nelze použít	MQZAO_SET_ ALL_CONTEXT **("6" na stránce 134)**
MQOO_SET	MQZAO_SET	Nelze použít	Bez kontroly
OPRÁVNĚNÍ UŽIVATELE MQOO_ALTERNATE_	**("9" na stránce 134)**	**("9" na stránce 134)**	MQZAO_ALTERNATE_ USER_AUTHORITY **("9" na stránce 134, "10" na stránce 134)**

Tabulka 12. Bezpečnostní autorizace potřebná pro volání MQPUT1			
Autorizace vyžadovaná pro:	**Objekt fronty ("1" na stránce 134)**	**Objekt procesu**	**Objekt správce front**
MQPMO_PASS_ IDENTITY_CONTEXT	MQZAO_PASS_ IDENTITY_CONTEXT **("11" na stránce 135)**	Nelze použít	Bez kontroly
MQPMO_PASS_ALL _CONTEXT	MQZAO_PASS_ ALL_CONTEXT **("11" na stránce 135)**	Nelze použít	Bez kontroly
MQPMO_SET_ IDENTITY_CONTEXT	MQZAO_SET_ IDENTITY_CONTEXT **("11" na stránce 135)**	Nelze použít	MQZAO_SET_ IDENTITY_CONTEXT **("6" na stránce 134)**

Tabulka 12. Bezpečnostní autorizace potřebná pro volání MQPUT1 (pokračování)			
Autorizace vyžadovaná pro:	**Objekt fronty ("1" na stránce 134)**	**Objekt procesu**	**Objekt správce front**
MQPMO_SET_ ALL_CONTEXT	MQZAO_SET_ ALL_CONTEXT **("11" na stránce 135)**	Nelze použít	MQZAO_SET_ ALL_CONTEXT **("6" na stránce 134)**
(Přenosová fronta) **("8" na stránce 134)**	MQZAO_SET_ ALL_CONTEXT	Nelze použít	MQZAO_SET_ ALL_CONTEXT **("6" na stránce 134)**
OPRÁVNĚNÍ UŽIVATELE MQPMO_ALTERNATE_	**("12" na stránce 135)**	Nelze použít	MQZAO_ALTERNATE_ USER_AUTHORITY **("10" na stránce 134)**

Tabulka 13. Bezpečnostní autorizace potřebná pro volání MQCLOSE			
Autorizace vyžadovaná pro:	**Objekt fronty ("1" na stránce 134)**	**Objekt procesu**	**Objekt správce front**
MQCO_DELETE	MQZAO_DELETE **("13" na stránce 135)**	Nelze použít	Nelze použít
MQCO_DELETE _PURGE	MQZAO_DELETE **("13" na stránce 135)**	Nelze použít	Nelze použít

Poznámky k tabulkám:

1. Při otevírání modelové fronty:
   - Pro modelovou frontu je kromě oprávnění k otevření modelové fronty pro typ přístupu, pro který otevíráte, zapotřebí oprávnění MQZAO_DISPLAY.
   - K vytvoření dynamické fronty není zapotřebí oprávnění MQZAO_CREATE.
   - Identifikátoru uživatele použitému k otevření modelové fronty jsou automaticky udělena všechna oprávnění specifická pro danou frontu (ekvivalent k MQZAO_ALL) pro vytvořenou dynamickou frontu.
2. Musí být zadána také hodnota MQOO_INPUT_ *. Toto je platné pro lokální, modelovou nebo alias frontu.
3. Tato kontrola se provádí pro všechny výstupní případy s výjimkou přenosových front (viz poznámka "8" na stránce 134).
4. Musí být uveden také parametr MQOO_OUTPUT.
5. MQOO_PASS_IDENTITY_CONTEXT je také odvozen z této volby.
6. Toto oprávnění je vyžadováno pro objekt správce front i pro konkrétní frontu.
7. MQOO_PASS_IDENTITY_CONTEXT, MQOO_PASS_ALL_CONTEXT a MQOO_SET_IDENTITY_CONTEXT jsou také odvozeny z této volby.
8. Tato kontrola se provádí pro lokální nebo modelovou frontu, která má atribut fronty *Usage* MQUS_TRANSMISSION, a otevírá se přímo pro výstup. Nepoužije se, pokud se otevírá vzdálená fronta (buď zadáním názvů vzdáleného správce front a vzdálené fronty, nebo zadáním názvu lokální definice vzdálené fronty).
9. Musí být zadán také alespoň jeden typ MQOO_INQUIRE (pro libovolný typ objektu) nebo MQOO_BROWSE, MQOO_INPUT_ *, MQOO_OUTPUT nebo MQOO_SET (pro fronty). Prováděná kontrola je stejná jako u ostatních zadaných voleb s použitím dodaného alternativního identifikátoru uživatele pro specifické oprávnění k objektu a aktuálního oprávnění aplikace pro kontrolu MQZAO_ALTERNATE_USER_IDENTIFIER.
10. Tato autorizace umožňuje zadat libovolné *AlternateUserId* .

11. Kontrola MQZAO_OUTPUT se provádí také v případě, že fronta nemá atribut fronty *Usage* s hodnotou MQUS_TRANSMISSION.
12. Provedená kontrola je stejně jako u ostatních zadaných voleb, s použitím dodaného alternativního identifikátoru uživatele pro specifické oprávnění fronty a aktuálního oprávnění aplikace pro kontrolu MQZAO_ALTERNATE_USER_IDENTIFIER.
13. Kontrola se provádí pouze v případě, že jsou pravdivá obě následující tvrzení:
    - Probíhá zavírání a odstraňování trvalé dynamické fronty.
    - Fronta nebyla vytvořena voláním MQOPEN , které vrátilo používaný popisovač objektu.

    V opačném případě není žádná kontrola.

ALW *Autorizace pro příkazy MQSC v řídicích PCF*

Tyto informace shrnují oprávnění potřebná pro každý příkaz MQSC obsažený v příkazu Escape PCF.

Nelze použít znamená, že tato operace není pro tento typ objektu relevantní.

ID uživatele, pod kterým je spuštěn program, který zadává příkaz, musí mít také následující oprávnění:

- Oprávnění MQZAO_CONNECT ke správci front
- Oprávnění MQZAO_DISPLAY pro správce front za účelem provádění příkazů PCF
- Oprávnění k zadání příkazu MQSC v textu příkazu Escape PCF

ALTER *objekt*

Objekt	**Je vyžadována autorizace**
Fronta	MQZAO_CHANGE
Téma	MQZAO_CHANGE
Proces	MQZAO_CHANGE
Správce front	MQZAO_CHANGE
Seznam názvů	MQZAO_CHANGE
Ověřovací informace	MQZAO_CHANGE
Kanál	MQZAO_CHANGE
Kanál připojení klienta	MQZAO_CHANGE
Modul listener	MQZAO_CHANGE
Služba	MQZAO_CHANGE
Informace o komunikaci	MQZAO_CHANGE

CLEAR *objekt*

Objekt	**Je vyžadována autorizace**
Fronta	MQZAO_CLEAR
Téma	MQZAO_CLEAR
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít
Ověřovací informace	Nelze použít
Kanál	Nelze použít

Objekt	Je vyžadována autorizace
Kanál připojení klienta	Nelze použít
Modul listener	Nelze použít
Služba	Nelze použít
Informace o komunikaci	Nelze použít

DEFINE *objekt* NOREPLACE (“1” na stránce 139)

Objekt	Je vyžadována autorizace
Fronta	MQZAO_CREATE **(“2” na stránce 139)**
Téma	MQZAO_CREATE **(“2” na stránce 139)**
Proces	MQZAO_CREATE **(“2” na stránce 139)**
Správce front	Nelze použít
Seznam názvů	MQZAO_CREATE **(“2” na stránce 139)**
Ověřovací informace	MQZAO_CREATE **(“2” na stránce 139)**
Kanál	MQZAO_CREATE **(“2” na stránce 139)**
Kanál připojení klienta	MQZAO_CREATE **(“2” na stránce 139)**
Modul listener	MQZAO_CREATE **(“2” na stránce 139)**
Služba	MQZAO_CREATE **(“2” na stránce 139)**
Informace o komunikaci	MQZAO_CREATE **(“2” na stránce 139)**

DEFINE *objekt* REPLACE (“1” na stránce 139, “3” na stránce 140)

Objekt	Je vyžadována autorizace
Fronta	MQZAO_CHANGE
Téma	MQZAO_CHANGE
Proces	MQZAO_CHANGE
Správce front	Nelze použít
Seznam názvů	MQZAO_CHANGE
Ověřovací informace	MQZAO_CHANGE
Kanál	MQZAO_CHANGE
Kanál připojení klienta	MQZAO_CHANGE
Modul listener	MQZAO_CHANGE
Služba	MQZAO_CHANGE
Informace o komunikaci	MQZAO_CHANGE

DELETE *objekt*

Objekt	Je vyžadována autorizace
Fronta	MQZAO_DELETE
Téma	MQZAO_DELETE

Objekt	Je vyžadována autorizace
Proces	MQZAO_DELETE
Správce front	Nelze použít
Seznam názvů	MQZAO_DELETE
Ověřovací informace	MQZAO_DELETE
Kanál	MQZAO_DELETE
Kanál připojení klienta	MQZAO_DELETE
Modul listener	MQZAO_DELETE
Služba	MQZAO_DELETE
Informace o komunikaci	MQZAO_DELETE

DISPLAY *objekt*

Objekt	Je vyžadována autorizace
Fronta	MQZAO_DISPLAY
Téma	MQZAO_DISPLAY
Proces	MQZAO_DISPLAY
Správce front	MQZAO_DISPLAY
Seznam názvů	MQZAO_DISPLAY
Ověřovací informace	MQZAO_DISPLAY
Kanál	MQZAO_DISPLAY
Kanál připojení klienta	MQZAO_DISPLAY
Modul listener	MQZAO_DISPLAY
Služba	MQZAO_DISPLAY
Informace o komunikaci	MQZAO_DISPLAY

START *objekt*

Objekt	Je vyžadována autorizace
Fronta	Nelze použít
Téma	Nelze použít
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít
Ověřovací informace	Nelze použít
Kanál	MQZAO_CONTROL
Kanál připojení klienta	Nelze použít
Modul listener	MQZAO_CONTROL
Služba	MQZAO_CONTROL

Objekt	Je vyžadována autorizace
Informace o komunikaci	Nelze použít

STOP *objekt*

Objekt	Je vyžadována autorizace
Fronta	Nelze použít
Téma	Nelze použít
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít
Ověřovací informace	Nelze použít
Kanál	MQZAO_CONTROL
Kanál připojení klienta	Nelze použít
Modul listener	MQZAO_CONTROL
Služba	MQZAO_CONTROL
Informace o komunikaci	Nelze použít

Příkazy kanálu

Příkaz	Objekt	Je vyžadována autorizace
Odeslat signál Ping pro kanál	Kanál	MQZAO_CONTROL
Resetovat kanál	Kanál	MQZAO_CONTROL_EXTENDED
Vyřešit kanál	Kanál	MQZAO_CONTROL_EXTENDED

Příkazy odběrů

Příkaz	Objekt	Je vyžadována autorizace
ALTER SUB	Téma	MQZAO_CONTROL
DEFINE SUB	Téma	MQZAO_CONTROL
ODSTRANIT SUB	Téma	MQZAO_CONTROL
DÍLČÍ ZOBRAZENÍ	Téma	MQZAO_DISPLAY

Příkazy pro zabezpečení

Příkaz	Objekt	Je vyžadována autorizace
SET AUTHREC	Správce front	MQZAO_CHANGE
DELETE AUTHREC-ODSTRANĚNÍ	Správce front	MQZAO_CHANGE
ZOBRAZIT ZÁZNAM OVĚŘENÍ	Správce front	MQZAO_DISPLAY
ZOBRAZENÍ AUTHSERV	Správce front	MQZAO_DISPLAY
ZOBRAZENÍ ENTAUTH	Správce front	MQZAO_DISPLAY
NASTAVIT CHLAUTH	Správce front	MQZAO_CHANGE

Příkaz	Objekt	Je vyžadována autorizace
ZOBRAZIT CHLAUTH	Správce front	MQZAO_DISPLAY
REFRESH SECURITY	Správce front	MQZAO_CHANGE

Stavové displeje

Příkaz	Objekt	Je vyžadována autorizace
ZOBRAZENÍ STAVU CHSTATUS	Správce front	MQZAO_DISPLAY Všimněte si, že v přenosové frontě je vyžadováno oprávnění `+inq` (nebo ekvivalentní oprávnění MQZAO_INQUIRE), pokud je typ kanálu CLUSSDR.
ZOBRAZENÍ STAVU LSSTATUS	Správce front	MQZAO_DISPLAY
ZOBRAZIT PUBSUB	Správce front	MQZAO_DISPLAY
ZOBRAZENÍ STAVU SBSTATUS	Správce front	MQZAO_DISPLAY
ZOBRAZENÍ STAVU SVSTATUS	Správce front	MQZAO_DISPLAY
ZOBRAZIT TPSTATUS	Správce front	MQZAO_DISPLAY

Příkazy klastru

Příkaz	Objekt	Je vyžadována autorizace
ZOBRAZENÍ SOUBORU CLUSQMGR	Správce front	MQZAO_DISPLAY
Aktualizovat klastr	Je vyžadováno členství ve skupině 'mqm'	
Reset klastru	Je vyžadováno členství ve skupině 'mqm'	
SUSPEND QMgr	Je vyžadováno členství ve skupině 'mqm'	
OBNOVTE SPRÁVCE FRONT	Je vyžadováno členství ve skupině 'mqm'	

Další administrativní příkazy

Příkaz	Objekt	Je vyžadována autorizace
PING QMGR	Správce front	MQZAO_DISPLAY
AKTUALIZOVAT SPRÁVCE FRONT	Správce front	MQZAO_CHANGE
RESET QMGR	Správce front	MQZAO_CHANGE
ZOBRAZENÍ PŘIPOJENÍ	Správce front	MQZAO_DISPLAY
STOP CONN	Správce front	MQZAO_CHANGE

Poznámka:

1. Pro příkazy DEFINE je oprávnění MQZAO_DISPLAY vyžadováno také pro objekt LIKE, pokud je zadán, nebo pro příslušný SYSTEM.DEFAULT.xxx , pokud je operátor LIKE vynechán.
2. Oprávnění MQZAO_CREATE není specifické pro konkrétní objekt nebo typ objektu. Oprávnění k vytvoření je uděleno pro všechny objekty pro určeného správce front zadáním typu objektu QMGR v příkazu `setmqaut` .

3. Toto platí, pokud objekt, který má být nahrazen, již existuje. Pokud tomu tak není, kontrola je jako u DEFINE *object* NOREPLACE.

Související informace

Klastrování: Využití doporučených postupů pro příkaz REFRESH CLUSTER

ALW *Autorizace pro příkazy PCF*

Tento oddíl shrnuje autorizace potřebné pro každý příkaz PCF.

Volba *Bez kontroly* znamená, že se neprovádí žádná kontrola autorizace. *Nelze použít* znamená, že tato operace není pro tento typ objektu relevantní.

ID uživatele, pod kterým je spuštěn program, který zadává příkaz, musí mít také následující oprávnění:

- Oprávnění MQZAO_CONNECT ke správci front
- Oprávnění MQZAO_DISPLAY pro správce front za účelem provádění příkazů PCF

Speciální autorizace MQZAO_ALL_ADMIN zahrnuje všechny autorizace v následujícím seznamu, které se vztahují k typu objektu, kromě MQZAO_CREATE, který není specifický pro konkrétní objekt nebo typ objektu.

Změnit *objekt*

Objekt	Je vyžadována autorizace
Fronta	MQZAO_CHANGE
Téma	MQZAO_CHANGE
Proces	MQZAO_CHANGE
správce front	MQZAO_CHANGE
Seznam názvů	MQZAO_CHANGE
Ověřovací informace	MQZAO_CHANGE
Kanál	MQZAO_CHANGE
Kanál připojení klienta	MQZAO_CHANGE
Modul listener	MQZAO_CHANGE
Služba	MQZAO_CHANGE
Informace o komunikaci	MQZAO_CHANGE

Vymazat *objekt*

Objekt	Je vyžadována autorizace
Fronta	MQZAO_CLEAR
Téma	MQZAO_CLEAR
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít
Ověřovací informace	Nelze použít
Kanál	Nelze použít
Kanál připojení klienta	Nelze použít
Modul listener	Nelze použít

Objekt	Je vyžadována autorizace
Služba	Nelze použít
Informace o komunikaci	Nelze použít

Kopírovat *objekt* (bez náhrady) (1)

Objekt	Je vyžadována autorizace
Fronta	MQZAO_CREATE **(2)**
Téma	MQZAO_CREATE **(2)**
Proces	MQZAO_CREATE **(2)**
Správce front	Nelze použít
Seznam názvů	MQZAO_CREATE **(2)**
Ověřovací informace	MQZAO_CREATE **(2)**
Kanál	MQZAO_CREATE **(2)**
Kanál připojení klienta	MQZAO_CREATE **(2)**
Modul listener	MQZAO_CREATE **(2)**
Služba	MQZAO_CREATE **(2)**
Informace o komunikaci	MQZAO_CREATE **(“2” na stránce 146)**

Kopírovat *objekt* (s nahrazením) (1, 4)

Objekt	Je vyžadována autorizace
Fronta	MQZAO_CHANGE
Téma	MQZAO_CHANGE
Proces	MQZAO_CHANGE
Správce front	Nelze použít
Seznam názvů	MQZAO_CHANGE
Ověřovací informace	MQZAO_CHANGE
Kanál	MQZAO_CHANGE
Kanál připojení klienta	MQZAO_CHANGE
Modul listener	MQZAO_CHANGE
Služba	MQZAO_CHANGE
Informace o komunikaci	MQZAO_CHANGE

Vytvořit *objekt* (bez náhrady) (3)

Objekt	Je vyžadována autorizace
Fronta	MQZAO_CREATE **(2)**
Téma	MQZAO_CREATE **(2)**
Proces	MQZAO_CREATE **(2)**
Správce front	Nelze použít

Objekt	Je vyžadována autorizace
Seznam názvů	MQZAO_CREATE **(2)**
Ověřovací informace	MQZAO_CREATE **(2)**
Kanál	MQZAO_CREATE **(2)**
Kanál připojení klienta	MQZAO_CREATE **(2)**
Modul listener	MQZAO_CREATE **(2)**
Služba	MQZAO_CREATE **(2)**
Informace o komunikaci	MQZAO_CREATE **(2)**

Vytvořte *objekt* (s nahrazením) (3, 4)

Objekt	Je vyžadována autorizace
Fronta	MQZAO_CHANGE
Téma	MQZAO_CHANGE
Proces	MQZAO_CHANGE
Správce front	Nelze použít
Seznam názvů	MQZAO_CHANGE
Ověřovací informace	MQZAO_CHANGE
Kanál	MQZAO_CHANGE
Kanál připojení klienta	MQZAO_CHANGE
Modul listener	MQZAO_CHANGE
Služba	MQZAO_CHANGE
Informace o komunikaci	MQZAO_CHANGE

Odstranit *objekt*

Objekt	Je vyžadována autorizace
Fronta	MQZAO_DELETE
Téma	MQZAO_DELETE
Proces	MQZAO_DELETE
Správce front	Nelze použít
Seznam názvů	MQZAO_DELETE
Ověřovací informace	MQZAO_DELETE
Kanál	MQZAO_DELETE
Kanál připojení klienta	MQZAO_DELETE
Modul listener	MQZAO_DELETE
Služba	MQZAO_DELETE
Informace o komunikaci	MQZAO_DELETE

Dotaz na *objekt*

Objekt	Je vyžadována autorizace
Fronta	MQZAO_DISPLAY
Téma	MQZAO_DISPLAY
Proces	MQZAO_DISPLAY
správce front	MQZAO_DISPLAY
Seznam názvů	MQZAO_DISPLAY
Ověřovací informace	MQZAO_DISPLAY
Kanál	MQZAO_DISPLAY
Kanál připojení klienta	MQZAO_DISPLAY
Modul listener	MQZAO_DISPLAY
Služba	MQZAO_DISPLAY
Informace o komunikaci	MQZAO_DISPLAY

Zjistit názvy *objektů*

Objekt	Je vyžadována autorizace
Fronta	Bez kontroly
Téma	Bez kontroly
Proces	Bez kontroly
Správce front	Bez kontroly
Seznam názvů	Bez kontroly
Ověřovací informace	Bez kontroly
Kanál	Bez kontroly
Kanál připojení klienta	Bez kontroly
Modul listener	Bez kontroly
Služba	Bez kontroly
Informace o komunikaci	Bez kontroly

Spustit *objekt*

Objekt	Je vyžadována autorizace
Fronta	Nelze použít
Téma	Nelze použít
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít
Ověřovací informace	Nelze použít
Kanál	MQZAO_CONTROL

Objekt	Je vyžadována autorizace
Kanál připojení klienta	Nelze použít
Modul listener	MQZAO_CONTROL
Služba	MQZAO_CONTROL
Informace o komunikaci	Nelze použít

Zastavit *objekt*

Objekt	Je vyžadována autorizace
Fronta	Nelze použít
Téma	Nelze použít
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít
Ověřovací informace	Nelze použít
Kanál	MQZAO_CONTROL
Kanál připojení klienta	Nelze použít
Modul listener	MQZAO_CONTROL
Služba	MQZAO_CONTROL
Informace o komunikaci	Nelze použít

Příkazy kanálu

Příkaz	Objekt	Je vyžadována autorizace
Odeslat signál Ping pro kanál	Kanál	MQZAO_CONTROL
Resetovat kanál	Kanál	MQZAO_CONTROL_EXTENDED
Vyřešit kanál	Kanál	MQZAO_CONTROL_EXTENDED

Příkazy odběrů

Příkaz	Objekt	Je vyžadována autorizace
Změnit odběr	Téma	MQZAO_CONTROL
Vytvořit odběr	Téma	MQZAO_CONTROL
Odstranit odběr	Téma	MQZAO_CONTROL
Zjistit odběr	Téma	MQZAO_DISPLAY

Příkazy pro zabezpečení

Příkaz	Objekt	Je vyžadována autorizace
Nastavit záznam oprávnění	Správce front	MQZAO_CHANGE
Odstranit záznam oprávnění	Správce front	MQZAO_CHANGE
Zjistit záznamy oprávnění	Správce front	MQZAO_DISPLAY

Příkaz	Objekt	Je vyžadována autorizace
Zjistit službu ověřování oprávnění	Správce front	MQZAO_DISPLAY
Zjistit oprávnění k entitě	Správce front	MQZAO_DISPLAY
Nastavit záznam ověření kanálu	Správce front	MQZAO_CHANGE
Zjistit záznam ověření kanálu	Správce front	MQZAO_DISPLAY
Aktualizovat zabezpečení	Správce front	MQZAO_CHANGE

Stavové displeje

Příkaz	Objekt	Je vyžadována autorizace
Zjistit stav kanálu	Správce front	MQZAO_DISPLAY Všimněte si, že v přenosové frontě je vyžadováno oprávnění `+inq` (nebo ekvivalentní oprávnění MQZAO_INQUIRE), pokud je typ kanálu CLUSSDR.
Stav modulu listener dotazování kanálu	Správce front	MQZAO_DISPLAY
Zjistit stav publikování/odběru	Správce front	MQZAO_DISPLAY
Stav dotazování odběru	Správce front	MQZAO_DISPLAY
Zjistit stav služby	Správce front	MQZAO_DISPLAY
Zjistit stav tématu	Správce front	MQZAO_DISPLAY

Příkazy klastru

Příkaz	Objekt	Je vyžadována autorizace
Zjistit správce front klastru	Správce front	MQZAO_DISPLAY
Aktualizovat klastr	Je vyžadováno členství ve skupině 'mqm'	Je vyžadováno členství ve skupině 'mqm'
Reset klastru	Je vyžadováno členství ve skupině 'mqm'	Je vyžadováno členství ve skupině 'mqm'
Pozastavit klastr správců front	Je vyžadováno členství ve skupině 'mqm'	Je vyžadováno členství ve skupině 'mqm'
Obnovit klastr správců front	Je vyžadováno členství ve skupině 'mqm'	Je vyžadováno členství ve skupině 'mqm'

Další administrativní příkazy

Příkaz	Objekt	Je vyžadována autorizace
Odeslat signál Ping pro správce front	Správce front	MQZAO_DISPLAY
Aktualizovat správce front	Správce front	MQZAO_CHANGE
Obnovit správce front	Správce front	MQZAO_CHANGE

Příkaz	Objekt	Je vyžadována autorizace
Obnovit statistiku front	Fronta	MQZAO_DISPLAY a MQZAO_CHANGE
Zjistit připojení	Správce front	MQZAO_DISPLAY
Zastavit připojení	Správce front	MQZAO_CHANGE

Poznámka:

1. Pro příkazy Copy je oprávnění MQZAO_DISPLAY také potřebné pro objekt From.
2. Oprávnění MQZAO_CREATE není specifické pro konkrétní objekt nebo typ objektu. Oprávnění k vytvoření je uděleno pro všechny objekty pro určeného správce front zadáním typu objektu QMGR v příkazu `setmqaut` .
3. Pro příkazy Create je také vyžadováno oprávnění MQZAO_DISPLAY pro příslušný systém SYSTEM.DEFAULT.* objekt.
4. Toto platí, pokud objekt, který má být nahrazen, již existuje. Pokud tomu tak není, je kontrola stejně jako pro Kopírovat nebo Vytvořit bez náhrady.

AIX Vytvoření a správa skupin v systému AIX

V systému AIX, pokud nepoužíváte službu NIS nebo NIS +, použijte SMITTY pro práci se skupinami.

Informace o této úloze

V systému AIXmůžete pomocí SMITTY vytvořit skupinu, přidat uživatele do skupiny, zobrazit seznam uživatelů, kteří jsou ve skupině, a odebrat uživatele ze skupiny.

Postup

1. V SMITTY vyberte **Zabezpečení a uživatelé** a stiskněte klávesu Enter.
2. Vyberte **Skupiny** a stiskněte klávesu Enter.
3. Chcete-li vytvořit skupinu, postupujte takto:
   a) Vyberte volbu **Přidat skupinu** a stiskněte klávesu Enter.
   b) Zadejte název skupiny a jména všech uživatelů, které chcete přidat do skupiny, oddělená čárkami.
   c) Stiskněte klávesu Enter pro vytvoření skupiny.
4. Chcete-li přidat uživatele do skupiny, postupujte takto:
   a) Vyberte **Změnit/zobrazit vlastnosti skupin** a stiskněte klávesu Enter.
   b) Zadejte název skupiny pro zobrazení seznamu členů skupiny.
   c) Přidejte jména uživatelů, které chcete přidat do skupiny, oddělená čárkami.
   d) Stiskněte klávesu Enter pro přidání názvů do skupiny.
5. Chcete-li zobrazit, kdo je ve skupině, postupujte takto:
   a) Vyberte **Změnit/zobrazit vlastnosti skupin** a stiskněte klávesu Enter.
   b) Zadejte název skupiny pro zobrazení seznamu členů skupiny.
6. Chcete-li odebrat uživatele ze skupiny, postupujte takto:
   a) Vyberte **Změnit/zobrazit vlastnosti skupin** a stiskněte klávesu Enter.
   b) Zadejte název skupiny pro zobrazení seznamu členů skupiny.
   c) Odstraňte jméno uživatele, kterého chcete odebrat ze skupiny.
   d) Stiskněte klávesu Enter pro odebrání názvu ze skupiny.

Linux Vytvoření a správa skupin v systému Linux

Pokud v systému Linuxnepoužíváte službu NIS nebo NIS +, použijte pro práci se skupinami soubor `/etc/group` .

Informace o této úloze

V systému Linuxjsou informace o skupině uloženy v souboru `/etc/group` . Pomocí příkazů můžete vytvořit skupinu, přidat uživatele do skupiny, zobrazit seznam uživatelů, kteří jsou ve skupině, a odebrat uživatele ze skupiny.

Postup

1. Chcete-li vytvořit novou skupinu, použijte příkaz **groupadd** .
   Zadejte následující příkaz:
   ```
   groupadd -g group-ID group-name
   ```
   kde *group-ID* je číselný identifikátor skupiny a *group-name* je název skupiny.
2. Chcete-li přidat člena do doplňkové skupiny, pomocí příkazu **usermod** zobrazte seznam doplňkových skupin, jejichž je uživatel momentálně členem, a doplňkových skupin, jejichž členem se má uživatel stát.
   Pokud je například uživatel již členem skupiny `groupaa` má se stát členem skupiny `groupb`, použijte tento příkaz:
   ```
   usermod -G groupa,groupb user-name
   ```
   kde *jméno-uživatele* je jméno uživatele.
3. Chcete-li zobrazit, kdo je členem skupiny, použijte příkaz **getent** .
   Zadejte následující příkaz:
   ```
   getent group group-name
   ```
   kde *název-skupiny* je název skupiny.
4. Chcete-li odebrat člena z doplňkové skupiny, pomocí příkazu **usermod** zobrazte seznam doplňkových skupin, jejichž členem má uživatel zůstat.
   Pokud je například primární skupina uživatele `users` a uživatel je také členem skupin `mqm`, `groupa` a `groupb`, použijte k odebrání uživatele ze skupiny `mqm` následující příkaz:
   ```
   usermod -G groupa,groupb user-name
   ```
   kde *jméno-uživatele* je jméno uživatele.

Windows Vytvoření a správa skupin v systému Windows

V systému Windowsmůžete pomocí funkce Správa počítače spravovat skupiny v počítači pracovní stanice nebo členského serveru.

Informace o této úloze

Pro řadiče domény jsou uživatelé a skupiny spravovány prostřednictvím Active Directory. Další podrobnosti o použití služby Active Directory naleznete v příslušných pokynech pro operační systém.

Veškeré změny provedené v členství činitele ve skupině nebudou rozpoznány, dokud nebude správce front restartován nebo dokud nezadáte příkaz MQSC **REFRESH SECURITY** (nebo ekvivalent PCF).

Panel Správa počítače Windows použijte pro práci s uživateli a skupinami. Změny provedené v aktuálně přihlášeném uživateli nemusí být účinné, dokud se uživatel znovu nepřihlásí.

Windows *Vytvoření skupiny v systému Windows*

Vytvořte skupinu pomocí ovládacího panelu.

Postup

1. Otevřít ovládací panel
2. Poklepejte na volbu **Nástroje pro správu**.
   Otevře se panel Nástroje pro správu.
3. Poklepejte na volbu **Správa počítače**.
   Otevře se panel Správa počítače.
4. Rozbalte volbu **Lokální uživatelé a skupiny**.
5. Klepněte pravým tlačítkem myši na položku **Skupiny**a vyberte volbu **Nová skupina ...**.
   Zobrazí se panel Nová skupina.
6. Do pole Název skupiny zadejte příslušný název a klepněte na tlačítko **Vytvořit**.
7. Klepněte na tlačítko **Zavřít**.

Windows *Přidání uživatele do skupiny v systému Windows*

Přidejte uživatele do skupiny pomocí ovládacího panelu.

Postup

1. Otevřít ovládací panel
2. Poklepejte na volbu **Nástroje pro správu**.
   Otevře se panel Nástroje pro správu.
3. Poklepejte na volbu **Správa počítače**.
   Otevře se panel Správa počítače.
4. Na panelu Správa počítače rozbalte položku **Místní uživatelé a skupiny**.
5. Vyberte volbu **Uživatelé** .
6. Poklepejte na uživatele, kterého chcete přidat do skupiny.
   Zobrazí se panel vlastností uživatele.
7. Vyberte kartu **Člen** .
8. Vyberte skupinu, do které chcete přidat uživatele. Pokud požadovaná skupina není viditelná:
   a) Klepněte na tlačítko **Přidat**.
      Zobrazí se panel Vybrat skupiny.
   b) Klepněte na volbu **Umístění ...**.
      Zobrazí se panel Umístění.
   c) Ze seznamu vyberte umístění skupiny, do které chcete přidat uživatele, a klepněte na tlačítko **OK**.
   d) Do uvedeného pole zadejte název skupiny.

      Případně klepněte na volbu **Rozšířené ...** a pak **Najít nyní** , abyste vypsali seznam skupin dostupných v aktuálně vybraném umístění. Zde vyberte skupinu, do které chcete přidat uživatele, a klepněte na tlačítko **OK**.
   e) Klepněte na tlačítko **OK**.
      Zobrazí se panel vlastností uživatele, který zobrazuje skupinu, kterou jste přidali.
   f) Vyberte skupinu.
9. Klepněte na tlačítko **OK**.
   Zobrazí se panel Správa počítače.

Windows *Zobrazení, kdo je ve skupině na Windows*

Zobrazte členy skupiny pomocí ovládacího panelu.

Postup

1. Otevřít ovládací panel
2. Poklepejte na volbu **Nástroje pro správu**.
   Otevře se panel Nástroje pro správu.
3. Poklepejte na volbu **Správa počítače**.
   Otevře se panel Správa počítače.
4. Na panelu Správa počítače rozbalte položku **Místní uživatelé a skupiny**.
5. Vyberte **Skupiny**.
6. Poklepejte na skupinu. Zobrazí se panel vlastností skupiny.
   Zobrazí se panel vlastností skupiny.

Výsledky

Zobrazí se členové skupiny.

Windows *Odebrání uživatele ze skupiny v systému Windows*

Odeberte uživatele ze skupiny pomocí ovládacího panelu.

Postup

1. Otevřít ovládací panel
2. Poklepejte na volbu **Nástroje pro správu**.
   Otevře se panel Nástroje pro správu.
3. Poklepejte na volbu **Správa počítače**.
   Otevře se panel Správa počítače.
4. Na panelu Správa počítače rozbalte položku **Místní uživatelé a skupiny**.
5. Vyberte volbu **Users** (Uživatelé).
6. Poklepejte na uživatele, kterého chcete přidat do skupiny.
   Zobrazí se panel vlastností uživatele.
7. Vyberte kartu **Člen** .
8. Vyberte skupinu, ze které chcete odebrat uživatele, a klepněte na tlačítko **Odebrat**.
9. Klepněte na tlačítko **OK**.
   Zobrazí se panel Správa počítače.

Výsledky

Nyní jste odebrali uživatele ze skupiny.

Windows Speciální aspekty zabezpečení na systému Windows

Některé funkce zabezpečení se v různých verzích produktu Windowschovají odlišně.

Zabezpečení produktu IBM MQ spoléhá na volání rozhraní API operačního systému pro informace o oprávněních uživatelů a členství ve skupinách. Některé funkce se v systémech Windows nechovají stejně. Tato kolekce témat obsahuje popisy toho, jak mohou tyto rozdíly ovlivnit zabezpečení produktu IBM MQ při spuštění produktu IBM MQ v prostředí Windows .

Windows *Lokální a doménové uživatelské účty pro službu IBM MQ Windows*

Produkt IBM MQ musí během své činnosti ověřovat, zda mají ke správcům front a frontám přístup pouze autorizovaní uživatelé. To vyžaduje speciální uživatelský účet, který může produkt IBM MQ použít k dotazování na informace o libovolném uživateli, který se o takový přístup pokouší.

- "Konfigurace speciálních uživatelských účtů pomocí konzoly Prepare IBM MQ Wizard" na stránce 150
- "Použití produktu IBM MQ s produktem Active Directory" na stránce 150
- "Uživatelská práva vyžadovaná pro službu IBM MQ Windows Service" na stránce 151

Konfigurace speciálních uživatelských účtů pomocí konzoly Prepare IBM MQ Wizard

Produkt Prepare IBM MQ Wizard vytvoří speciální uživatelský účet, aby mohla být služba Windows sdílena procesy, které ji potřebují používat (viz téma Konfigurace IBM MQ s produktem PPrepare IBM MQ Wizard).

Služba Windows je sdílena mezi procesy klienta pro instalaci produktu IBM MQ . Pro každou instalaci se vytvoří jedna služba. Každá služba má název `MQ_`*`InstallationName`*a zobrazovaný název `IBM MQ(`*`InstallationName`*`)`.

Protože každá služba musí být sdílena mezi neinteraktivními a interaktivními relacemi přihlášení, musíte ji spustit pod speciálním uživatelským účtem. Můžete použít jeden speciální uživatelský účet pro všechny služby nebo vytvořit různé speciální uživatelské účty. Každý speciální uživatelský účet musí mít právo uživatele `Přihlásit se jako služba`, další informace viz Tabulka 14 na stránce 151. Pokud ID uživatele nemá oprávnění ke spuštění služby, služba se nespustí a vrátí chybu v protokolu systémových událostí Windows . Obvykle budete mít spuštěnou databázi Prepare IBM MQ Wizarda správně nastavíte ID uživatele. Pokud jste však nakonfigurovali ID uživatele ručně, je možné, že budete mít problém, který budete muset vyřešit.

Když nainstalujete produkt IBM MQ a spustíte produkt Prepare IBM MQ Wizard poprvé, vytvoří lokální uživatelský účet pro službu s názvem MUSR_MQADMIN s požadovanými nastaveními a oprávněními, včetně `Přihlášení jako služba`.

Pro následné instalace produkt Prepare IBM MQ Wizard vytvoří uživatelský účet s názvem MUSR_MQADMIN*x*, kde *x* je další dostupné číslo představující ID uživatele, které neexistuje. Heslo pro MUSR_MQADMIN*x* se náhodně vygeneruje při vytvoření účtu a použije se ke konfiguraci přihlašovacího prostředí pro službu. Generovanému heslu nevyprší platnost.

Tento účet IBM MQ není ovlivněn žádnými zásadami účtu, které jsou nastaveny na systému, aby vyžadovaly změnu hesel účtu po určité době.

Heslo není známé mimo toto jednorázové zpracování a je uloženo operačním systémem Windows v zabezpečené části registru.

Použití produktu IBM MQ s produktem Active Directory

V některých konfiguracích sítě, kde jsou uživatelské účty definovány na řadičích domény, které používají adresářovou službu Active Directory , nemusí mít lokální uživatelský účet, pod kterým běží produkt IBM MQ , oprávnění, které vyžaduje k dotazování na členství ve skupinách jiných uživatelských účtů domény. Když instalujete produkt IBM MQ, produkt Prepare IBM MQ Wizard identifikuje, zda se jedná o tento případ, provedením testů a dotazem na konfiguraci sítě.

Pokud lokální uživatelský účet, pod kterým běží produkt IBM MQ , nemá požadované oprávnění, produkt Prepare IBM MQ Wizard vás vyzve k zadání podrobností účtu uživatelského účtu domény s konkrétními uživatelskými právy. Informace o vytvoření a nastavení účtu domény systému Windows naleznete v tématu Vytvoření a nastavení účtů domény systému Windows pro produkt IBM MQ. Uživatelská práva, která uživatelský účet domény vyžaduje, viz Tabulka 14 na stránce 151.

Když jste zadali platné podrobnosti o účtu uživatele domény do Prepare IBM MQ Wizard, průvodce nakonfiguruje službu IBM MQ Windows , aby se spustila pod novým účtem. Podrobnosti o účtu jsou uloženy v zabezpečené části registru a uživatelé je nemohou číst.

Když je služba spuštěna, spustí se služba IBM MQ Windows a zůstane spuštěna po celou dobu, kdy je služba spuštěna. Administrátor systému IBM MQ , který se přihlásí k serveru po spuštění služby Windows , může produkt IBM MQ Explorer použít k administraci správců front na serveru. Tím se produkt IBM MQ Explorer připojí k existujícímu procesu služby Windows . Tyto dvě akce vyžadují různé úrovně oprávnění, než budou moci pracovat:

- Proces spuštění vyžaduje oprávnění ke spuštění.
- Administrátor produktu IBM MQ vyžaduje přístupové oprávnění.

Uživatelská práva vyžadovaná pro službu IBM MQ Windows Service

V následující tabulce jsou uvedena uživatelská práva požadovaná pro lokální a doménové uživatelské účty, pod nimiž je spuštěna služba Windows pro instalaci produktu IBM MQ .

Tabulka 14. Uživatelská práva požadovaná pro službu systému Windows IBM MQ

Oprávnění	**Popis**
Přihlásit se jako dávková úloha	Povolí spuštění služby IBM MQ Windows pod tímto uživatelským účtem.
Přihlásit jako služba.	Umožňuje uživatelům nastavit službu IBM MQ Windows pro přihlášení pomocí nakonfigurovaného účtu.
Vypnout systém	Umožňuje službě IBM MQ Windows restartovat server, je-li to nakonfigurováno, když dojde k selhání obnovy služby.
Zvýšit kvóty	Nezbytné pro volání operačního systému `CreateProcessAsUser` .
Vystupovat jako část operačního systému	Nezbytné pro volání operačního systému `LogonUser` .
Vynechat kontrolu průchodu	Nezbytné pro volání operačního systému `LogonUser` .
Zaměnit úroveň procesu	Nezbytné pro volání operačního systému `LogonUser` .

Poznámka: Práva k ladicím programům mohou být potřebná v prostředích, kde jsou spuštěny aplikace ASP a IIS.

Váš uživatelský účet domény musí mít tato uživatelská práva Windows nastavena jako efektivní uživatelská práva, jak jsou uvedena v aplikaci Lokální zásady zabezpečení. Pokud nejsou, nastavte je buď pomocí aplikace Lokální zásada zabezpečení lokálně na serveru, nebo pomocí aplikace Zabezpečení domény v celé doméně.

Windows *Windows Oprávnění zabezpečení serveru*

Instalace produktu IBM MQ se na serveru Windows chová odlišně v závislosti na tom, zda lokální uživatel nebo uživatel domény provádí instalaci.

Pokud *lokální* uživatel nainstaluje IBM MQ, agent Prepare IBM MQ Wizard zjistí, že lokální uživatel vytvořený pro službu IBM MQ Windows může načíst informace o skupinovém členství uživatele, který provedl instalaci. Produkt Prepare IBM MQ Wizard se zeptá uživatele na konfiguraci sítě, aby zjistil, zda jsou na řadičích domény spuštěných na systému Windows 2000 nebo novějším definovány jiné uživatelské účty. Pokud ano, musí být služba produktu IBM MQ Windows spuštěna pod účtem uživatele domény s konkrétními nastaveními a oprávněními. Prepare IBM MQ Wizard vyzve uživatele k zadání podrobností o účtu tohoto uživatele, jak je popsáno v tématu Konfigurace IBM MQ s Prepare IBM MQ Wizard.

Pokud *uživatel domény* nainstaluje IBM MQ, agent Prepare IBM MQ Wizard zjistí, že lokální uživatel vytvořený pro službu IBM MQ Windows nemůže načíst informace o skupinovém členství uživatele, který provedl instalaci. V tomto případě produkt Prepare IBM MQ Wizard vždy vyzve uživatele k zadání podrobností účtu účtu uživatele domény, který má služba IBM MQ Windows používat.

Když služba IBM MQ Windows potřebuje použít uživatelský účet domény, IBM MQ nemůže správně fungovat, dokud nebude nakonfigurován pomocí Prepare IBM MQ Wizard. Produkt Prepare IBM MQ Wizard nepovoluje uživateli pokračovat s jinými úlohami, dokud nebude služba Windows nakonfigurována s vhodným účtem.

Další informace naleznete v tématu Vytvoření a nastavení účtů domény pro produkt IBM MQ.

Windows *Změna jména uživatele přidruženého ke službě IBM MQ*

Jméno uživatele přidružené ke službě IBM MQ můžete změnit vytvořením nového účtu a zadáním jeho podrobností pomocí Prepare IBM MQ Wizard.

Informace o této úloze

Když poprvé nainstalujete produkt IBM MQ a spustíte produkt Prepare IBM MQ Wizard , vytvoří lokální uživatelský účet pro službu s názvem MUSR_MQADMIN. Pro následné instalace produkt Prepare IBM MQ Wizard vytvoří uživatelský účet s názvem MUSR_MQADMIN*x*, kde *x* je další dostupné číslo představující ID uživatele, které neexistuje.

Možná budete muset změnit jméno uživatele přidružené ke službě IBM MQ z MUSR_MQADMIN nebo MUSR_MQADMIN*x* na něco jiného. To může být třeba provést například v případě, že je váš správce front přidružen k produktu Db2, který nepřijímá jména uživatelů delší než 8 znaků.

Postup

1. Vytvořte nový uživatelský účet (například **NEW_NAME**).
2. Použijte Prepare IBM MQ Wizard k zadání podrobností nového uživatelského účtu.

Související úlohy

Konfigurace produktu IBM MQ pomocí konzoly Prepare IBM MQ Wizard

Windows *Změna hesla lokálního uživatelského účtu služby IBM MQ Windows*

Heslo lokálního uživatelského účtu služby IBM MQ Windows můžete změnit pomocí panelu Správa počítače.

Informace o této úloze

Chcete-li změnit heslo lokálního uživatelského účtu služby IBM MQ Windows , postupujte takto:

Postup

1. Identifikujte uživatele, pod kterým je služba spuštěna.
2. Zastavte službu IBM MQ z panelu Správa počítače.
3. Změňte požadované heslo stejným způsobem, jako byste změnili heslo jednotlivce.
4. Přejděte na vlastnosti pro službu IBM MQ z panelu Správa počítače.
5. Vyberte stránku **Přihlášení** .
6. Potvrďte, že uvedený název účtu odpovídá uživateli, pro kterého bylo heslo upraveno.
7. Zadejte heslo do polí **Heslo** a **Potvrdit heslo** a klepněte na tlačítko **OK**.

Windows *Změna hesla pro službu IBM MQ Windows pro instalaci spuštěnou pod uživatelským účtem domény*

Jako alternativu k použití konzoly Prepare IBM MQ Wizard k zadání podrobností o účtu uživatele domény můžete použít panel Správa počítače ke změně podrobností **Přihlášení** pro službu IBM MQ specifickou pro instalaci.

Informace o této úloze

Pokud je služba produktu IBM MQ Windows pro instalaci spuštěna pod účtem uživatele domény, můžete změnit heslo pro účet takto:

Postup

1. Změňte heslo pro účet domény na řadiči domény. Možná budete muset požádat administrátora domény, aby to provedl za vás.
2. Chcete-li upravit stránku **Přihlášení** pro službu IBM MQ , postupujte takto.
   a) Identifikujte uživatele, pod kterým je služba spuštěna.
   b) Zastavte službu IBM MQ z panelu Správa počítače.
   c) Změňte požadované heslo stejným způsobem, jako byste změnili heslo jednotlivce.
   d) Přejděte na vlastnosti pro službu IBM MQ z panelu Správa počítače.
   e) Vyberte stránku **Přihlášení** .
   f) Potvrďte, že uvedený název účtu odpovídá uživateli, pro kterého bylo heslo upraveno.
   g) Zadejte heslo do polí **Heslo** a **Potvrdit heslo** a klepněte na tlačítko **OK**.

   Uživatelský účet, pod kterým je spuštěna služba produktu IBM MQ Windows , provádí všechny příkazy MQSC vydané aplikacemi uživatelského rozhraní nebo prováděné automaticky při spuštění systému, ukončení práce systému nebo při obnově služby. Tento uživatelský účet proto musí mít administrátorská práva IBM MQ . Standardně je přidán do lokální skupiny mqm na serveru. Pokud je toto členství odebráno, služba IBM MQ Windows nefunguje. Další informace o uživatelských právech viz “Uživatelská práva vyžadovaná pro službu IBM MQ Windows Service” na stránce 151.

   Pokud se vyskytne problém zabezpečení s uživatelským účtem, pod kterým je spuštěna služba IBM MQ Windows , objeví se v protokolu systémových událostí chybové zprávy a popisy.

Související úlohy

Konfigurace produktu IBM MQ pomocí konzoly Prepare IBM MQ Wizard

Windows *Aspekty při povýšení serverů Windows na řadiče domény*

Při povýšení serveru Windows na řadič domény byste měli zvážit, zda je vhodné nastavení zabezpečení týkající se oprávnění uživatelů a skupin. Při změně stavu počítače Windows mezi serverem a řadičem domény byste měli vzít v úvahu, že to může ovlivnit operaci IBM MQ , protože IBM MQ používá lokálně definovanou skupinu mqm.

Nastavení zabezpečení týkající se uživatelů domény a oprávnění skupiny

Produkt IBM MQ při implementaci zásady zabezpečení spoléhá na informace o členství ve skupinách, což znamená, že je důležité, aby ID uživatele, který provádí operace produktu IBM MQ , mohlo určovat členství ostatních uživatelů ve skupinách.

Když povyšujete server Windows na řadič domény, zobrazí se vám volba pro nastavení zabezpečení týkající se oprávnění uživatelů a skupin. Tato volba řídí, zda jsou libovolní uživatelé schopni načíst členství ve skupinách ze služby Active Directory. Je-li řadič domény nastaven tak, aby lokální účty měly oprávnění dotazovat se na členství ve skupinách uživatelských účtů domény, výchozí ID uživatele vytvořené produktem IBM MQ během procesu instalace může získat členství ve skupinách pro ostatní uživatele podle potřeby. Je-li však řadič domény nastaven tak, aby lokální účty neměly oprávnění dotazovat se na členství ve skupinách uživatelských účtů domény, brání to produktu IBM MQ v dokončení kontroly, zda

jsou uživatelé definovaní v doméně autorizováni pro přístup ke správcům front nebo frontám a přístup se nezdaří. Pokud používáte produkt Windows na řadiči domény, který byl nastaven tímto způsobem, musí být použit speciální uživatelský účet domény s požadovanými oprávněními.

V tomto případě musíte vědět:

- Jak se chovají oprávnění zabezpečení pro vaši verzi produktu Windows .
- Jak povolit členům skupiny domain mqm číst členství ve skupinách.
- Jak nakonfigurovat službu IBM MQ Windows pro spuštění pod uživatelem domény.

Další informace naleznete v tématu Konfigurace uživatelských účtů pro produkt IBM MQ.

IBM MQ přístup k lokální skupině mqm

Když jsou servery Windows povýšeny na řadiče domény nebo z nich vyřazeny, produkt IBM MQ ztratí přístup k lokální skupině mqm.

Je-li server povýšen na řadič domény, obor se změní z lokálního na lokální. Když je počítač degradován na server, všechny lokální skupiny domény jsou odebrány. To znamená, že změna počítače ze serveru na řadič domény a zpět na server ztratí přístup k lokální skupině mqm. Příznakem je chyba označující nedostatek lokální skupiny mqm, například:

```
>crtmqm qm0
AMQ8066:Local mqm group not found.
```

Chcete-li tento problém odstranit, znovu vytvořte lokální skupinu mqm pomocí standardních nástrojů pro správu systému Windows . Vzhledem k tomu, že všechny informace o členství ve skupině jsou ztraceny, musíte znovu uvést privilegované uživatele IBM MQ do nově vytvořené lokální skupiny mqm. Pokud je počítač členem domény, musíte také přidat skupinu domain mqm do lokální skupiny mqm, abyste udělili oprávněným doménovým IBM MQ ID uživatelů požadovanou úroveň oprávnění.

Windows *Omezení vnořených skupin v systému Windows*

Existují omezení pro použití vnořených skupin. Tyto výsledky částečně vyplývají z úrovně funkčnosti domény a částečně z omezení IBM MQ .

Active Directory může podporovat různé typy skupin v kontextu domény v závislosti na úrovni funkčnosti domény. Standardně se domény Windows 2003 nacházejí v " Windows 2000 smíšená " úroveň funkčnosti. (Windows Server 2008 a Windows Server 2012 postupujte podle modelu domény Windows 2003 .) Úroveň funkčnosti domény určuje podporované typy skupin a úroveň vnoření povolené při konfiguraci ID uživatelů v prostředí domény. Podrobné informace o rozsahu skupiny a kritériích zahrnutí naleznete v dokumentaci ke službě Active Directory .

Kromě požadavků Active Directory jsou na ID používaná produktem IBM MQuvalena další omezení. Síťová rozhraní API používaná produktem IBM MQ nepodporují všechny konfigurace podporované úrovní funkčnosti domény. Výsledkem je, že produkt IBM MQ není schopen dotazovat se na členství ve skupinách libovolných ID domén přítomných ve skupině Domain Local, která je poté vnořena do lokální skupiny. Kromě toho není podporováno vícenásobné vnoření globálních a univerzálních skupin. Jsou však podporovány okamžitě vnořené globální nebo univerzální skupiny.

Windows *Autorizace uživatelů ke vzdálenému použití produktu IBM MQ*

Potřebujete-li vytvořit a spustit správce front při vzdáleném připojení k produktu IBM MQ , musíte mít uživatelský přístup `Vytvořit globální objekty` .

Informace o této úloze

Poznámka: Administrátoři mají standardně přístup uživatele `Vytvořit globální objekty` , takže pokud jste administrátor, můžete vytvořit a spustit správce front při vzdáleném připojení bez změny uživatelských práv.

Pokud se připojujete k počítači se systémem Windows pomocí Terminálové služby nebo Připojení ke vzdálené ploše a máte problémy s vytvářením, spouštěním nebo odstraňováním správce front, může to být způsobeno tím, že nemáte uživatelský přístup `Vytvořit globální objekty`.

Uživatelský přístup `Vytvořit globální objekty` omezuje uživatele, kteří jsou autorizováni vytvářet objekty v globálním prostoru jmen. Aby mohla aplikace vytvořit globální objekt, musí být buď spuštěna v globálním prostoru jmen, nebo musí mít uživatel, pod kterým je aplikace spuštěna, použitý uživatelský přístup `Vytvořit globální objekty` .

Pokud se vzdáleně připojujete k počítači se systémem Windows pomocí služby Terminal Services nebo nástroje Připojení ke vzdálené ploše, aplikace se spouštějí ve vlastním lokálním prostoru jmen. Pokusíte-li se vytvořit nebo odstranit správce front pomocí příkazu IBM MQ Explorer nebo **crtmqm** či **dltmqm** nebo chcete-li spustit správce front pomocí příkazu **strmqm** , dojde k selhání autorizace. Tím se vytvoří IBM MQ FDC s ID zkoušky XY132002.

Spuštění správce front pomocí produktu IBM MQ Explorernebo pomocí příkazu **amqmdain qmgr start** funguje správně, protože tyto příkazy přímo nespouštějí správce front. Namísto toho příkazy odešlou požadavek na spuštění správce front do samostatného procesu spuštěného v globálním oboru názvů.

Pokud různé metody administrace produktu IBM MQ při použití terminálových služeb nefungují, zkuste nastavit uživatelské právo `Vytvořit globální objekty` .

Postup

1. Otevřete panel Nástroje pro správu:

   Windows Server 2008 a Windows Server 2012
   Přistupte k tomuto panelu pomocí **Ovládací panely** > **Systém a údržba** > **Nástroje pro správu**.

   Windows 8.1
   Přístup k tomuto panelu pomocí **Nástroje pro správu** > **Správa počítače**
2. Poklepejte na položku **Lokální zásada zabezpečení**.
3. Rozbalte **Lokální zásady**.
4. Klepněte na volbu **Přiřazení práv uživatele**.
5. Přidejte nového uživatele nebo skupinu do zásady `Vytvořit globální objekty` .

Windows *Uživatelský program kanálu SSPI v systému Windows*

Produkt IBM MQ for Windows dodává program uživatelské procedury zabezpečení, který lze použít pro kanály zpráv i MQI. Uživatelská procedura je dodávána jako zdrojový a objektový kód a poskytuje jednosměrné a obousměrné ověření.

Uživatelská procedura zabezpečení používá rozhraní SSPI (Security Support Provider Interface), které poskytuje integrované prostředky zabezpečení platforem Windows .

Uživatelská procedura zabezpečení poskytuje následující služby identifikace a ověření:

jednosměrné ověření
Používá podporu ověřování NTLM (Windows NT LAN Manager). NTLM umožňuje serverům ověřit své klienty. Neumožňuje klientovi ověřit server nebo jeden server ověřit jiný. NTLM byl navržen pro síťové prostředí, ve kterém jsou servery považovány za originální. NTLM je podporováno na všech platformách Windows , které jsou podporovány produktem IBM WebSphere MQ 7.0.

Tato služba se obvykle používá v kanálu MQI k povolení správce front serveru pro ověřování aplikace IBM MQ MQI client . Klientská aplikace je identifikována ID uživatele přidruženým ke spuštěným procesům.

Chcete-li provést ověření, uživatelská procedura zabezpečení na straně klienta kanálu získá token ověření od správce NTLM a odešle token ve zprávě zabezpečení svému partnerovi na druhém konci kanálu. Uživatelská procedura zabezpečení partnera předá token správci NTLM, který zkontroluje, zda je token autentický. Není-li uživatelská procedura zabezpečení partnera spokojena s autenticitou tokenu, instruuje agenta MCA, aby kanál uzavřel.

Obousměrná nebo vzájemná autentizace

Používá ověřovací služby Kerberos . Protokol Kerberos nepředpokládá, že servery v síťovém prostředí jsou skutečné. Servery mohou ověřovat klienty a jiné servery a klienti mohou ověřovat servery. Kerberos je podporován na všech platformách Windows , které jsou podporovány produktem IBM WebSphere MQ 7.0.

Tuto službu lze použít pro kanály zpráv i MQI. V kanálu zpráv poskytuje vzájemné ověření dvou správců front. V kanálu MQI umožňuje, aby se správce front serveru a aplikace IBM MQ MQI client navzájem ověřovaly. Správce front je identifikován svým názvem s předponou s řetězcem `ibmMQSeries/`. Klientská aplikace je identifikována ID uživatele přidruženým ke spuštěným procesům.

Chcete-li provést vzájemné ověření, inicializační uživatelská procedura zabezpečení získá token ověření ze serveru zabezpečení Kerberos a odešle token ve zprávě zabezpečení svému partnerovi. Uživatelská procedura zabezpečení partnera předá token serveru Kerberos , který zkontroluje, zda je autentický. Server zabezpečení Kerberos vygeneruje druhý token, který partner odešle ve zprávě zabezpečení do inicializační uživatelské procedury zabezpečení. Inicializační uživatelská procedura zabezpečení poté požádá server Kerberos o kontrolu, zda je druhý token autentický. Pokud během této výměny není některá uživatelská procedura zabezpečení spokojena s autenticitou tokenu odeslaného druhou, instruuje agenta MCA, aby kanál zavřel.

Uživatelská procedura zabezpečení je dodána ve formátu zdroje i objektu. Zdrojový kód můžete použít jako výchozí bod pro psaní vlastních programů uživatelské procedury kanálu nebo můžete použít modul objektu tak, jak byl dodán. Objektový modul má dva vstupní body, jeden pro jednosměrné ověřování pomocí podpory ověřování NTLM a druhý pro dvousměrné ověřování pomocí ověřovacích služeb Kerberos .

Další informace o fungování uživatelského programu kanálu SSPI a pokyny, jak jej implementovat, naleznete v tématu Použití uživatelské procedury zabezpečení SSPI na Windows systémech.

Windows *Použití souborů šablon zabezpečení v systému Windows*

Použití šablony může ovlivnit nastavení zabezpečení použité pro soubory a adresáře IBM MQ . Pokud použijete vysoce zabezpečenou šablonu, použijte ji před instalací produktu IBM MQ.

Produkt Windows podporuje textové soubory šablon zabezpečení, které lze použít k použití jednotného nastavení zabezpečení pro jeden nebo více počítačů s modulem snap-in Konfigurace zabezpečení a analýza konzoly MMC. Společnost Windows dodává zejména několik šablon, které zahrnují řadu nastavení zabezpečení s cílem poskytnout specifické úrovně zabezpečení. Mezi tyto šablony patří kompatibilní, zabezpečené a vysoce zabezpečené.

Použití jedné z těchto šablon může ovlivnit nastavení zabezpečení použité pro soubory a adresáře IBM MQ . Chcete-li použít šablonu Highly Secure, nakonfigurujte počítač před instalací produktu IBM MQ.

Pokud použijete vysoce zabezpečenou šablonu na počítač, na kterém je již nainstalován produkt IBM MQ , všechna oprávnění, která jste nastavili v souborech a adresářích IBM MQ , se odeberou. Vzhledem k tomu, že tato oprávnění byla odebrána, ztratíte oprávnění *Administrátor*, *mqm*a v případě potřeby přístup skupiny *Všichni* z chybových adresářů.

Windows *Konfigurace dalšího oprávnění pro Windows aplikace, které se připojují k IBM MQ*

Účet, pod kterým jsou spuštěny procesy IBM MQ , může vyžadovat další autorizaci, než bude možné udělit přístup k aplikačním procesům SYNCHRONIZOVAT.

Informace o této úloze

Můžete se setkat s problémy, pokud máte aplikace Windows , například stránky ASP, které se připojují k produktu IBM MQ a jsou nakonfigurované tak, aby se spouštěly na vyšší úrovni zabezpečení, než je obvyklé.

Produkt IBM MQ vyžaduje přístup SYNC k procesům aplikace, aby bylo možné koordinovat určité akce. Když se aplikace serveru poprvé pokusí připojit ke správci front, IBM MQ upraví proces tak, aby

administrátorům produktu IBM MQ udělil oprávnění SYNCHRONIZOVAT. Avšak účet, pod kterým běží procesy IBM MQ , může vyžadovat další autorizaci, než bude možné udělit požadovaný přístup.

Chcete-li konfigurovat další oprávnění pro ID uživatele, pod kterým jsou spuštěny procesy IBM MQ , postupujte takto:

Postup

1. Spusťte nástroj Lokální zásada zabezpečení, klepněte na volbu **Nastavení zabezpečení**->**Lokální zásady**->**Přiřazení uživatelských práv**, klepněte na volbu **Ladit programy**.
2. Poklepejte na volbu **Ladit programy**a poté přidejte ID uživatele IBM MQ do seznamu.

   Pokud je systém v doméně Windows a platné nastavení zásad stále není nastaveno, i když je nastaveno lokální nastavení zásad, musí být ID uživatele autorizováno stejným způsobem na úrovni domény pomocí nástroje Zásady zabezpečení domény.

IBM i Nastavení zabezpečení na systému IBM i

Zabezpečení v systému IBM i je implementováno pomocí zabezpečení na úrovni objektů IBM MQ Object Authority Manager (OAM) a IBM i .

Aspekty zabezpečení, které musí být provedeny při určování přístupových oprávnění k objektům IBM MQ .

Při nastavování oprávnění pro uživatele ve vašem podniku je třeba vzít v úvahu následující body:

1. Udělte a zrušte oprávnění k příkazům IBM MQ for IBM i pomocí příkazů IBM i GRTOBJAUT a RVKOBJAUT .

   V knihovně QMQM jsou určité nepříkazové (* cmd) objekty nastaveny tak, aby měly ***PUBLIC** oprávnění k ***USE**. Neměňte oprávnění těchto objektů nebo použijte seznam oprávnění k poskytnutí oprávnění. Jakákoli nesprávná oprávnění mohou ohrozit funkčnost produktu IBM MQ .
2. Během instalace produktu IBM MQ for IBM ijsou vytvořeny následující speciální profily uživatelů:

   QMQM
   Používá se především pro interní funkce pouze pro produkty. Lze jej však použít ke spouštění důvěryhodných aplikací pomocí příkazu MQCNO_FASTPATH_BINDINGS. Viz Připojení ke správci front pomocí volání MQCONNX.

   QMQMADM
   Používá se jako profil skupiny pro administrátory produktu IBM MQ. Profil skupiny poskytuje přístup k příkazům CL a prostředkům IBM MQ .

   Při použití SBMJOB k zadání programů, které volají příkazy IBM MQ , nesmí být USER explicitně nastaveno na QMQMADM. Místo toho nastavte USER na QMQM nebo jiný profil uživatele, který má jako skupinu zadáno QMQMADM.
3. Odesíláte-li příkazy kanálu vzdáleným správcům front, zkontrolujte, zda je váš profil uživatele členem skupiny QMQMADM v cílovém systému. Seznam příkazů kanálu PCF a MQSC viz IBM MQ for IBM i CL příkazy.
4. Sada skupin přidružená k uživateli se uloží do mezipaměti, když jsou autorizace skupin vypočteny pomocí OAM.

   Veškeré změny provedené v členstvích skupin uživatele po uložení sady skupin do mezipaměti nebudou rozpoznány, dokud nerestartujete správce front nebo dokud neprovedete příkaz RFRMQMAUT pro obnovení zabezpečení.
5. Omezte počet uživatelů, kteří mají oprávnění pracovat s příkazy, které jsou obzvláště citlivé. Mezi tyto příkazy patří:

   - Vytvořit správce front zpráv (CRTMQM)
   - Odstranit správce front zpráv (DLTMQM)
   - Spuštění správce front zpráv (STRMQM)
   - Ukončení správce front zpráv (ENDMQM)

- Spuštění příkazového serveru (STRMQMCSVR)
- Ukončení příkazového serveru (ENDMQMCSVR)

6. Definice kanálů obsahují specifikaci programu uživatelské procedury zabezpečení. Vytvoření a úprava kanálu vyžaduje speciální aspekty. Podrobnosti o uživatelských procedur zabezpečení jsou uvedeny v části "Přehled uživatelské procedury zabezpečení" na stránce 110.
7. Programy uživatelské procedury kanálu a monitoru spouštěčů mohou být nahrazeny. Za bezpečnost těchto výměn odpovídá programátor.

IBM i Správce oprávnění k objektu na systému IBM i

Správce oprávnění k objektům (OAM) spravuje oprávnění uživatelů k manipulaci s objekty IBM MQ , včetně front a definic procesů. Také poskytuje příkazové rozhraní, jehož prostřednictvím můžete udělit nebo odvolat přístupová oprávnění k objektu pro určitou skupinu uživatelů. Rozhodnutí o povolení přístupu k prostředku je provedeno modulem OAM a po tomto rozhodnutí následuje správce front. Pokud modul OAM nemůže provést rozhodnutí, správce front zabrání přístupu k tomuto prostředku.

Prostřednictvím OAM můžete ovládat:

- Přístup k objektům IBM MQ prostřednictvím rozhraní MQI. Když se aplikační program pokusí o přístup k objektu, OAM zkontroluje, zda má profil uživatele provádějící požadavek autorizaci pro požadovanou operaci.

  To zejména znamená, že fronty a zprávy ve frontách mohou být chráněny před neoprávněným přístupem.
- Oprávnění k použití příkazů PCF a MQSC.

Různé skupiny uživatelů mohou mít různá přístupová oprávnění ke stejnému objektu. Například pro specifickou frontu může jedna skupina provádět operace vložení i získání; jiná skupina může mít povoleno pouze procházet frontu (MQGET s volbou procházení). Podobně některé skupiny mohou mít oprávnění k získání a vložení do fronty, ale nemohou ji měnit nebo odstraňovat.

Příkazy systému IBM MQ for IBM i a provádění operací s objekty systému IBM MQ for IBM i .

IBM i IBM MQ oprávnění na IBM i

Pro přístup k objektům IBM MQ potřebujete oprávnění k zadání příkazu a k přístupu k odkazovanému objektu. Administrátoři mají přístup ke všem prostředkům IBM MQ .

Přístup k objektům IBM MQ je řízen oprávněními k:

1. Zadejte příkaz IBM MQ .
2. Přístup k objektům IBM MQ , na které odkazuje příkaz

Všechny CL příkazy IBM MQ for IBM i jsou dodávány s vlastníkem QMQM a profil administrace (QMQMADM) má práva *USE s přístupem *PUBLIC nastaveným na *EXCLUDE.

Poznámka: Program QSRDUPER používá instalační program licencovaného programu IBM MQ for IBM i k duplikaci objektů příkazu (*CMD) v knihovně QSYS. V produktu IBM i V5R4 a novějším byl program QSRDUPER změněn tak, aby výchozí chování bylo vytvořit příkaz proxy namísto duplikátu původního příkazu. Příkaz proxy přesměruje provedení příkazu na jiný příkaz a má atribut PRX. Pokud příkaz proxy se stejným názvem jako kopírovaný příkaz existuje v knihovně QSYS, soukromá oprávnění k příkazu proxy nejsou udělena příkazu v knihovně produktu. Pokusí se zobrazit výzvu nebo spustit příkaz proxy v knihovně QSYS a zkontrolovat oprávnění cílového příkazu v knihovně produktu. Jakékoli změny oprávnění k objektům *CMD proto musí být provedeny v knihovně produktu (QMQM) a ty v knihovně QSYS nemusí být upraveny. Příklad:

```
GRTOBJAUT OBJ(QMQM/DSPMQMQ) OBJTYPE(*CMD) USER(MQUSER) AUT(*USE)
```

Změny struktury oprávnění některých CL příkazů produktu umožňují veřejné použití těchto příkazů, pokud máte požadované oprávnění OAM k objektům IBM MQ k provedení těchto změn.

Chcete-li být IBM MQ administrátorem produktu IBM i, musíte být členem *skupiny QMQMADM*. Tato skupina má vlastnosti podobné vlastnostem skupiny mqm na systémech AIX, Linux, and Windows . Skupina QMQMADM je vytvořena zejména při instalaci produktu IBM MQ for IBM ia členové skupiny QMQMADM mají přístup ke všem prostředkům produktu IBM MQ v systému. Máte také přístup ke všem prostředkům IBM MQ , pokud máte oprávnění *ALLOBJ.

Administrátoři mohou k administraci produktu IBM MQpoužívat příkazy CL. Jedním z těchto příkazů je GRTMQMAUT, který se používá k udělení oprávnění ostatním uživatelům. Jiný příkaz STRMQMMQSC umožňuje administrátorovi zadávat příkazy MQSC lokálnímu správci front.

Související pojmy

“Oprávnění ke správě IBM MQ v systému IBM i” na stránce 90

IBM i *Přístupová oprávnění pro objekty IBM MQ na IBM i*

Přístupová oprávnění požadovaná pro spuštění CL příkazů IBM MQ .

Produkt IBM MQ for IBM i kategorizuje příkazy CL produktu do dvou skupin:

Skupina 1

Uživatelé musí být ve skupině uživatelů QMQMADM nebo musí mít oprávnění *ALLOBJ, aby mohli tyto příkazy zpracovat. Uživatelé, kteří mají kterékoli z těchto oprávnění, mohou zpracovat všechny příkazy ve všech kategoriích bez nutnosti dalšího oprávnění.

Poznámka: Tato oprávnění přepisují jakákoli oprávnění OAM.

Tyto příkazy lze seskupit takto:

- Příkazy příkazového serveru
  - ENDMQMCSVR, Ukončit příkazový server IBM MQ
  - STRMQMCSVR, Spuštění příkazového serveru IBM MQ
- Příkaz obslužné rutiny fronty nedoručených zpráv
  - STRMQMDLQ, Spustit IBM MQ obslužnou rutinu fronty nedoručených zpráv
- Příkaz modulu listener
  - Listener ENDMQMLSR, ukončení IBM MQ
  - STRMQMLSR, Spuštění neobjektového modulu listener
- Příkazy obnovy médií
  - RCDMQMIMG, Záznam IBM MQ obrazu objektu
  - RCRMQMOBJ, Znovu vytvořit objekt IBM MQ
  - WRKMQMTRN, Práce s IBM MQ Q-transakcemi
- Příkazy správce front
  - CRTMQM, Vytvořit správce front zpráv
  - DLTMQM, Odstranění správce front zpráv
  - ENDMQM, Ukončit správce front zpráv
  - STRMQM, Spuštění správce front zpráv
- Příkazy pro zabezpečení
  - GRTMQMAUT, udělení oprávnění k objektu IBM MQ
  - RVKMQMAUT, Odvolání oprávnění k objektu IBM MQ
- Příkaz trasování
  - TRCMQM, úloha trasování IBM MQ
- Příkazy pro transakce
  - RSVMQMTRN, Vyřešit IBM MQ transakci

- Příkazy monitoru spouštěčů
  - STRMQMTRM, Spuštění monitoru spouštěčů
- IBM MQPříkazy SC
  - RUNMQSC, Spuštění příkazů IBM MQSC
  - STRMQMMQSC, Spuštění příkazů IBM MQSC

Skupina 2

Zbývající příkazy, pro které jsou vyžadovány dvě úrovně oprávnění:

1. Oprávnění IBM i ke spuštění příkazu. Administrátor systému IBM MQ toto nastaví pomocí příkazu **GRTOBJAUT** , aby potlačil omezení *PUBLIC (*EXCLUDE) pro uživatele nebo skupinu uživatelů.

   Příklad:

   ```
   GRTOBJAUT OBJ(QMQM/DSPMQMQ) OBJTYPE(*CMD) USER(MQUSER) AUT(*USE)
   ```

2. IBM MQ oprávnění k manipulaci s objekty IBM MQ přidruženými k příkazu nebo příkazům, které má správné oprávnění IBM i v kroku 1.

   Toto oprávnění je řízeno uživatelem, který má odpovídající oprávnění OAM pro požadovanou akci, nastavenou administrátorem produktu IBM MQ pomocí příkazu **GRTMQMAUT** .

   Příklad:

   ```
   GRTMQMAUT *connect authority to the queue manager + *admchg authority to
           the queue
   ```

Příkazy lze seskupit takto:

- Příkazy kanálu
  - CHGMQMCHL, změna kanálu IBM MQ

    To vyžaduje oprávnění * pro připojení ke správci front a oprávnění * admchg ke kanálu.
  - CPYMQMCHL, Kopírovat kanál IBM MQ

    To vyžaduje oprávnění * connect a * admcrt ke správci front, oprávnění * admdsp k výchozímu typu kanálu, který má být zkopírován, a oprávnění * admcrt ke třídě objektů kanálu.

    Například kopírování odesílacího kanálu vyžaduje oprávnění * admdsp do SYSTEM.DEF.SENDER
  - CRTMQMCHL, Vytvořit kanál IBM MQ

    To vyžaduje oprávnění * connect a * admcrt ke správci front, oprávnění * admdsp k výchozímu typu kanálu, který má být vytvořen, a oprávnění * admcrt ke třídě objektů kanálu.

    Například vytvoření odesílacího kanálu vyžaduje oprávnění * admdsp pro SYSTEM.DEF.SENDER
  - DLTMQMCHL, odstranění kanálu IBM MQ

    To vyžaduje oprávnění * k připojení ke správci front a oprávnění * admdlt ke kanálu.
  - RSVMQMCHL, Vyřešit IBM MQ kanál

    To vyžaduje oprávnění * k připojení ke správci front a oprávnění * ctrlx ke kanálu.
- Příkazy pro zobrazení

  Chcete-li zpracovat příkazy DSP, musíte udělit uživateli oprávnění `*connect` a `*admdsp` ke správci front spolu se všemi uvedenými specifickými volbami:
  - DSPMQM, Zobrazení správce front zpráv
  - DSPMQMAUT, Zobrazení oprávnění k objektu IBM MQ
  - DSPMQMAUTI, Zobrazení IBM MQ ověřovacích informací- `*admdsp` k objektu ověřovacích informací

  - DSPMQMCHL, Zobrazení IBM MQ kanálu- *admdsp pro kanál
  - DSPMQMCSVR, Zobrazení příkazového serveru IBM MQ
  - DSPMQMNL, Zobrazit IBM MQ Seznam názvů- *admdsp do seznamu názvů
  - DSPMQMOBJN, Zobrazení IBM MQ názvů objektů
  - DSPMQMPRC, zobrazení IBM MQ Process- *admdsp pro proces
  - DSPMQMQ, Zobrazení IBM MQ fronty- *admdsp do fronty
  - DSPMQMTOP, Zobrazit IBM MQ Téma- *admdsp k tématu
- Práce s příkazy

  Chcete-li zpracovat příkazy WRK a zobrazit panel voleb, musíte správci front udělit oprávnění uživatele *connect a *admdsp spolu se všemi uvedenými specifickými volbami:

  - WRKMQM, Práce se správci front zpráv
  - WRKMQMAUT, Práce s oprávněním k objektu IBM MQ
  - WRKMQMAUTD, Práce s daty oprávnění k objektu IBM MQ
  - WRKMQMAUTI, Práce s ověřovacími informacemi IBM MQ
    - *admchg pro příkaz Změnit objekt ověřovacích informací IBM MQ .
    - *admcrt pro příkaz Vytvořit a kopírovat IBM MQ objekt ověřovacích informací.
    - *admdlt pro příkaz Odstranit objekt ověřovacích informací IBM MQ .
    - *admdsp pro příkaz Display IBM MQ Authentication Information Object.
  - WRKMQMCHL, Práce s kanálem IBM MQ

    To vyžaduje následující oprávnění:

    - *admchg pro příkaz Změnit kanál IBM MQ .
    - *admclr pro příkaz Vymazat kanál IBM MQ .
    - *admcrt pro příkaz Vytvořit a kopírovat IBM MQ kanál.
    - *admdlt pro příkaz Odstranit IBM MQ kanál.
    - *admdsp pro příkaz Display IBM MQ Channel.
    - *ctrl pro příkaz Spustit IBM MQ kanál.
    - *ctrl pro příkaz Ukončit kanál IBM MQ .
    - *ctrl pro příkaz Ping IBM MQ Channel.
    - *ctrlx pro příkaz Reset IBM MQ Channel.
    - *ctrlx pro příkaz Vyřešit IBM MQ kanál.
  - WRKMQMCHST, Práce se stavem kanálu IBM MQ

    To vyžaduje oprávnění *admdsp ke kanálu.
  - WRKMQMCL, Práce s klastry IBM MQ
  - WRKMQMCLQ, Práce s IBM MQ frontami klastru
  - WRKMQMCLQM, Práce se správcem front klastru IBM MQ
  - WRKMQMLSR, Práce s modulem listener IBM MQ
  - WRKMQMMSG, Práce se zprávami IBM MQ

    To vyžaduje oprávnění *browse k frontě
  - WRKMQMNL, Práce se seznamu názvů IBM MQ

    To vyžaduje následující oprávnění:

    - *admchg pro příkaz Change IBM MQ Namelist.
    - *admcrt pro příkaz Vytvořit a kopírovat IBM MQ seznam názvů.

- *admdlt pro příkaz Odstranit IBM MQ seznam názvů.
- *admdsp pro příkaz Display IBM MQ Namelist.

– WRKMQMPRC, Práce s procesy IBM MQ

To vyžaduje následující oprávnění:

- *admchg pro příkaz Proces změny IBM MQ .
- *admcrt pro příkaz Create and Copy IBM MQ Process.
- *admdlt pro příkaz Delete IBM MQ Process.
- *admdsp pro příkaz IBM MQ Zobrazit proces.

– WRKMQMQ, Práce s frontami IBM MQ

To vyžaduje následující oprávnění:

- *admchg pro příkaz Změnit IBM MQ frontu.
- *admclr pro příkaz Vymazat IBM MQ frontu.
- *admcrt pro příkaz Vytvořit a kopírovat IBM MQ frontu.
- *admdlt pro příkaz Odstranit IBM MQ frontu.
- *admdsp pro příkaz Zobrazení IBM MQ fronty.

– WRKMQMQSTS, Práce se stavem fronty IBM MQ

– WRKMQMTOP, Práce s IBM MQ tématy

To vyžaduje následující oprávnění

- *admchg pro příkaz Změnit téma IBM MQ .
- *admcrt pro příkaz Create and Copy IBM MQ Topic.
- *admdlt pro příkaz Odstranit IBM MQ téma.
- *admdsp pro příkaz Display IBM MQ Topic.

– WRKMQMSUB, Práce s odběry IBM MQ

• Další příkazy kanálu

Chcete-li zpracovat příkazy kanálu, musíte uživateli udělit specifická uvedená oprávnění:

– ENDMQMCHL, ukončení IBM MQ kanálu

To vyžaduje oprávnění *connect ke správci front a oprávnění *allmqi k přenosové frontě přidružené ke kanálu.

– ENDMQMLSR, Ukončit modul listener IBM MQ

To vyžaduje oprávnění *connect ke správci front a oprávnění *ctrl k uvedenému objektu modulu listener.

– PNGMQMCHL, Ping IBM MQ kanál

To vyžaduje oprávnění *connect a *inq ke správci front a oprávnění *ctrl k objektu kanálu.

– RSTMQMCHL, resetování kanálu IBM MQ

To vyžaduje oprávnění *connect ke správci front.

– STRMQMCHL, Spuštění kanálu IBM MQ

To vyžaduje oprávnění *connect ke správci front a oprávnění *ctrl k objektu kanálu.

– STRMQMCHLI, Spuštění IBM MQ inicializátoru kanálu

To vyžaduje oprávnění *connect a *inq ke správci front a oprávnění *allmqi k inicializační frontě přidružené k přenosové frontě kanálu.

– STRMQMLSR, Spuštění modulu listener IBM MQ

To vyžaduje oprávnění * k připojení ke správci front a oprávnění * ctrl k pojmenovanému objektu modulu listener.

- Další příkazy:

  Chcete-li zpracovat následující příkazy, musíte uživateli udělit specifická uvedená oprávnění:

  – CCTMQM, připojení ke správci front zpráv

    To nevyžaduje žádné oprávnění k objektu IBM MQ .

  – CHGMQM, Změna správce front zpráv

    To vyžaduje oprávnění `*connect` a `*admchg` ke správci front.

  – CHGMQMAUTI, Změna ověřovacích informací IBM MQ

    To vyžaduje oprávnění `*connect` ke správci front a oprávnění `*admchg` a `*admdsp` k objektu ověřovacích informací.

  – CHGMQMNL, Změnit seznam názvů IBM MQ

    To vyžaduje oprávnění `*connect` ke správci front a oprávnění `*admchg` k seznamu názvů.

  – CHGMQMPRC, proces změny IBM MQ

    To vyžaduje oprávnění `*connect` ke správci front a oprávnění `*admchg` k procesu.

  – CHGMQMQ, Změna fronty IBM MQ

    To vyžaduje oprávnění `*connect` ke správci front a oprávnění `*admchg` ke frontě.

  – CLRMQMQ, Vymazat frontu IBM MQ

    To vyžaduje oprávnění `*connect` ke správci front a oprávnění `*admclr` ke frontě.

  – CPYMQMAUTI, Kopírovat ověřovací informace IBM MQ

    To vyžaduje oprávnění `*connect` ke správci front a oprávnění `*admdsp` k objektu ověřovacích informací a oprávnění `*admcrt` ke třídě objektu ověřovacích informací.

  – CPYMQMNL, Kopírovat IBM MQ seznam názvů

    To vyžaduje oprávnění `*connect` a `*admcrt` ke správci front.

  – CPYMQMPRC, proces kopírování IBM MQ

    To vyžaduje oprávnění `*connect` a `*admcrt` ke správci front.

  – CPYMQMQ, Kopírovat frontu IBM MQ

    To vyžaduje oprávnění `*connect` a `*admcrt` ke správci front.

  – CRTMQMAUTI, Vytvořit IBM MQ ověřovací informace

    To vyžaduje oprávnění `*connect` ke správci front a oprávnění `*admdsp` k objektu ověřovacích informací a oprávnění `*admcrt` ke třídě objektu ověřovacích informací.

  – CRTMQMNL, Vytvořit IBM MQ seznam názvů

    To vyžaduje oprávnění `*connect` a `*admcrt` ke správci front a oprávnění `*admdsp` k výchozímu seznamu názvů.

  – CRTMQMPRC, vytvoření IBM MQ procesu

    To vyžaduje oprávnění `*connect` a `*admcrt` ke správci front a oprávnění `*admdsp` k výchozímu procesu.

  – CRTMQMQ, vytvořit frontu IBM MQ

    To vyžaduje oprávnění `*connect` a `*admcrt` ke správci front a oprávnění `*admdsp` k výchozí frontě.

  – CVTMQMDTA, příkaz pro převod IBM MQ datového typu

    To nevyžaduje žádné oprávnění k objektu IBM MQ .

  – DLTMQMAUTI, Odstranění ověřovacích informací IBM MQ

To vyžaduje oprávnění *connect ke správci front a oprávnění *ctrlx k objektu ověřovacích informací.

– DLTMQMNL, Odstranit seznam názvů IBM MQ

  To vyžaduje oprávnění *connect ke správci front a oprávnění *admdlt k seznamu názvů.

– Proces DLTMQMPRC, odstranění IBM MQ

  To vyžaduje oprávnění *connect ke správci front a oprávnění *admdlt k procesu.

– DLTMQMQ, Odstranit IBM MQ frontu

  To vyžaduje oprávnění *connect ke správci front a oprávnění *admdlt ke frontě.

– DSCMQM, odpojení od správce front zpráv

  To nevyžaduje žádné oprávnění k objektu IBM MQ .

– RFRMQMAUT, aktualizace zabezpečení

  To vyžaduje oprávnění *connect ke správci front.

– RFRMQMCL, aktualizace klastru

  To vyžaduje oprávnění *connect ke správci front.

– RSMMQMCLQM, Obnovit správce front klastru

  To vyžaduje oprávnění *connect ke správci front.

– RSTMQMCL, Resetování klastru

  To vyžaduje oprávnění *connect ke správci front.

– SPDMQMCLQM, Pozastavit správce front klastru

  To vyžaduje oprávnění *connect ke správci front.

IBM i *Autorizace přístupu na systému IBM i*

Pomocí těchto informací porozumíte příkazům autorizace přístupu.

Autorizace definované klíčovým slovem AUT v příkazech GRTMQMAUT a RVKMQMAUT lze kategorizovat takto:

- Autorizace související s voláními MQI
- Příkazy administrace související s autorizací
- Autorizace kontextu
- Obecná oprávnění, tj. pro volání MQI, pro příkazy nebo obojí.

V následujících tabulkách jsou uvedena různá oprávnění s použitím parametru AUT pro volání MQI, kontextová volání, příkazy MQSC a PCF a generické operace.

Tabulka 15. Autorizace pro volání MQI

Testovaná aplikace	**Popis**
*ALTUSR	Povolit použití oprávnění jiného uživatele pro volání MQOPEN a MQPUT1 .
*BROWSE	Načtěte zprávu z fronty zadáním volání MQGET s volbou BROWSE.
*CONNECT	Připojte aplikaci k určenému správci front zadáním volání MQCONN.
*GET	Načtení zprávy z fronty vyvoláním volání MQGET.
*INQ	Zadáním volání MQINQ proveďte dotaz na specifickou frontu.
*PUB	Chcete-li publikovat zprávu pomocí volání MQPUT, otevřete téma.
*PUT	Vložte zprávu do specifické fronty zadáním volání MQPUT.

Tabulka 15. Autorizace pro volání MQI (pokračování)	
Testovaná aplikace	**Popis**
*RESUME	Obnovte odběr pomocí volání MQSUB.
*SET	Nastavte atributy ve frontě z rozhraní MQI zadáním volání MQSET. Pokud otevřete frontu pro více voleb, musíte být autorizováni pro každou z nich.
*SUB	Vytvořit, pozměnit nebo obnovit odběr tématu pomocí volání MQSUB.

Tabulka 16. Autorizace pro kontextová volání	
Testovaná aplikace	**Popis**
*PASSALL	Předat veškerý kontext v uvedené frontě. Všechna pole kontextu se zkopírují z původního požadavku.
*PASSID	Předejte kontext identity do uvedené fronty. Kontext identity je stejný jako u požadavku.
*SETALL	Nastavte všechny kontexty v určené frontě. To je používáno speciálními systémovými obslužnými programy.
*SETID	Nastavte kontext identity v určené frontě. To je používáno speciálními systémovými obslužnými programy.

Tabulka 17. Autorizace pro volání MQSC a PCF	
Testovaná aplikace	**Popis**
*ADMCHG	Změňte atributy uvedeného objektu.
*ADMCLR	Vymazat uvedený objekt (pouze příkaz PCF Vymazat objekt).
*ADMCRT	Vytvořte objekty uvedeného typu.
*ADMDLT	Odstranit uvedený objekt.
*ADMDSP	Zobrazí atributy uvedeného objektu.

Tabulka 18. Oprávnění pro generické operace	
Testovaná aplikace	**Popis**
*ALL	Použijte všechny operace použitelné pro objekt. Oprávnění `all` je ekvivalentní sjednocení oprávnění `alladm`, `allmqia` `system` odpovídajících typu objektu.
*ALLADM	Proveďte všechny operace administrace použitelné pro daný objekt.
*ALLMQI	Použijte všechna volání MQI použitelná pro objekt.
*CTRL	Řízení spouštění a ukončování kanálů, listenerů a služeb.
*CTRLX	Vynulujte pořadové číslo a vyřešte neověřené kanály.

IBM i *Použití příkazů autorizace přístupu na systému IBM i*

Tyto informace použijte, chcete-li se dozvědět více o příkazech autorizace přístupu a použít příklady příkazů.

Použití příkazu GRTMQMAUT

Máte-li požadovanou autorizaci, můžete pomocí příkazu GRTMQMAUT udělit oprávnění profilu uživatele nebo skupině uživatelů pro přístup ke konkrétnímu objektu. Následující příklady ilustrují použití příkazu GRTMQMAUT :

1. ```
   GRTMQMAUT OBJ(RED.LOCAL.QUEUE) OBJTYPE(*LCLQ) USER(GROUPA) +
             AUT(*BROWSE *PUT) MQMNAME('saturn.queue.manager')
   ```

   V tomto příkladu platí následující:

   - RED.LOCAL.QUEUE je název objektu.
   - *LCLQ (lokální fronta) je typ objektu.
   - GROUPA je název profilu uživatele v systému, jehož oprávnění se mají změnit. Tento profil lze použít jako skupinový profil pro ostatní uživatele.
   - *BROWSE a *PUT jsou autorizace, které se udělují určené frontě.

     Produkt *BROWSE přidává autorizaci k procházení zpráv ve frontě (k vydání příkazu MQGET s volbou procházení).

     Produkt *PUT přidává autorizaci pro vložení zpráv (MQPUT) do fronty.
   - saturn.queue.manager je název správce front.
2. Následující příkaz udělí uživatelům JACK a JILL všechny použitelné autorizace pro všechny definice procesů pro výchozího správce front.

   ```
   GRTMQMAUT OBJ(*ALL) OBJTYPE(*PRC) USER(JACK JILL) AUT(*ALL)
   ```
3. Následující příkaz udělí uživateli oprávnění GEORGE vložit zprávu do fronty ORDERSve správci front TRENT.

   ```
   GRTMQMAUT OBJ(TRENT) OBJTYPE(*MQM) USER(GEORGE) AUT(*CONNECT) MQMNAME (TRENT)
   GRTMQMAUT OBJ(ORDERS) OBJTYPE(*Q) USER(GEORGE) AUT(*PUT) MQMNAME (TRENT)
   ```

Použití příkazu RVKMQMAUT

Máte-li požadovanou autorizaci, můžete pomocí příkazu RVKMQMAUT odebrat dříve udělenou autorizaci profilu uživatele nebo skupiny uživatelů pro přístup ke konkrétnímu objektu. Následující příklady ilustrují použití příkazu RVKMQMAUT :

1. ```
   RVKMQMAUT OBJ(RED.LOCAL.QUEUE) OBJTYPE(*LCLQ) USER(GROUPA) +
   AUT(*PUT) MQMNAME('saturn.queue.manager')
   ```

   Oprávnění pro vložení zpráv do uvedené fronty, které bylo uděleno v předchozím příkladu, je odebráno pro GROUPA.
2. ```
   RVKMQMAUT OBJ(PAY*) OBJTYPE(*Q) USER(*PUBLIC) AUT(*GET) +
   MQMNAME(PAYROLLQM)
   ```

   Oprávnění k získávání zpráv z libovolné fronty s názvem začínajícím znaky PAY, vlastněné správcem front PAYROLLQM, je odebráno všem uživatelům systému, pokud tito uživatelé nebo skupina, do které patří, nebyli autorizováni odděleně.
   ```

Použití příkazu DSPMQMAUT

Zobrazení oprávnění MQM (DSPMQMAUT) Příkaz zobrazí pro uvedený objekt a uživatele seznam oprávnění, která má uživatel pro objekt. Následující příklad ukazuje, jak se příkaz používá:

```
DSPMQMAUT OBJ(ADMINNL) OBJTYPE(*NMLIST) USER(JOE) OUTPUT(*PRINT) +
MQMNAME(ADMINQM)
```

Použití příkazu RFRMQMAUT

Aktualizace zabezpečení MQM (RFRMQMAUT) umožňuje okamžitě aktualizovat informace o skupině autorizace OAM, což odráží změny provedené na úrovni operačního systému, aniž by bylo nutné zastavit a restartovat správce front. Následující příklad ukazuje, jak se příkaz používá:

```
RFRMQMAUT MQMNAME(ADMINQM)
```

IBM i Tabulky specifikace autorizace na systému IBM i

Pomocí těchto informací můžete určit, jaká autorizace je vyžadována pro použití konkrétních volání rozhraní API a konkrétních voleb těchto volání pro objekty front, objekty procesů a objekty správce front.

Tabulky specifikace autorizace začínající v produktu Tabulka 19 na stránce 168 přesně definují, jak autorizace fungují, a omezení, která platí. Tabulky platí pro tyto situace:

- Aplikace, které volají rozhraní MQI
- Administrační programy, které vydávají příkazy MQSC jako řídicí PCF
- Administrační programy, které vydávají příkazy PCF

V této sekci jsou informace prezentovány jako sada tabulek, které určují následující data:

Akce, která se má provést
Volba MQI, příkaz MQSC nebo příkaz PCF.

Objekt řízení přístupu
Fronta, definice procesu, správce front, seznam názvů, kanál, kanál připojení klienta, modul listener, služba nebo objekt ověřovacích informací.

Je vyžadována autorizace
Vyjádřeno jako konstanta MQZAO_.

V tabulkách konstanty s předponou MQZAO_ odpovídají klíčovým slovům v seznamu oprávnění pro příkazy **GRTMQMAUT** a **RVKMQMAUT** pro konkrétní entitu. Například MQZAO_BROWSE odpovídá klíčovému slovu *BROWSE ; podobně klíčové slovo MQZAO_SET_ALL_CONTEXT odpovídá klíčovému slovu *SETALLatd. Tyto konstanty jsou definovány v hlavičkovém souboru cmqzc.h, který je dodáván s produktem.

Autorizace MQI

Aplikace může vydávat specifická volání a volby MQI pouze v případě, že identifikátoru uživatele, pod kterým je spuštěna (nebo jehož autorizací lze předpokládat), byla udělena příslušná autorizace.

Čtyři volání MQI vyžadují kontroly autorizace: MQCONN, MQOPEN, MQPUT1a MQCLOSE.

V případě MQOPEN a MQPUT1je provedena kontrola oprávnění pro název otevíraného objektu, a nikoli pro název či názvy, což bude mít za následek vyřešení názvu. Aplikaci lze například udělit oprávnění k otevření alias fronty, aniž by měla oprávnění k otevření základní fronty, do které se alias převádí. Pravidlem je, že kontrola se provádí u první definice zjištěné během procesu rozpoznávání názvů, který není aliasem správce front, pokud není definice aliasu správce front otevřena přímo; to znamená, že její název se zobrazí v poli *ObjectName* deskriptoru objektu. Oprávnění je vždy potřebné pro otevření konkrétního objektu; v některých případech je vyžadováno další oprávnění nezávislé na frontě, získané prostřednictvím autorizace pro objekt správce front.

Tabulka 19 na stránce 168, Tabulka 20 na stránce 168, Tabulka 21 na stránce 169a Tabulka 22 na stránce 169 shrnují autorizace potřebné pro každé volání.

Poznámka: Tyto tabulky neuvádějí seznamy názvů, kanály, kanály připojení klienta, listenery, služby nebo objekty ověřovacích informací. Důvodem je, že na tyto objekty se nevztahuje žádná z autorizací, s výjimkou oprávnění MQOO_INQUIRE, pro která platí stejná autorizace jako pro ostatní objekty.

Tabulka 19. Bezpečnostní autorizace potřebná pro volání MQCONN

Autorizace vyžadovaná pro:	**Objekt fronty ("1" na stránce 169)**	**Objekt procesu**	**Objekt správce front**
Volba MQCONN	Nelze použít	Nelze použít	MQZAO_CONNECT

Tabulka 20. Bezpečnostní autorizace potřebná pro volání MQOPEN

Autorizace vyžadovaná pro:	**Objekt fronty ("1" na stránce 169)**	**Objekt procesu**	**Objekt správce front**
MQOO_DOTAZOVAT	MQZAO_INQUIRE **("2" na stránce 170)**	MQZAO_INQUIRE **("2" na stránce 170)**	MQZAO_INQUIRE **("2" na stránce 170)**
MQOO_BROWSE	MQZAO_BROWSE	Nelze použít	Bez kontroly
MQOO_INPUT_ *	MQZAO_INPUT	Nelze použít	Bez kontroly
MQOO_SAVE_ ALL_CONTEXT **("3" na stránce 170)**	MQZAO_INPUT	Nelze použít	Nelze použít
MQOO_OUTPUT (normální fronta) **("4" na stránce 170)**	MQZAO_OUTPUT	Nelze použít	Nelze použít
MQOO_PASS_ IDENTITY_CONTEXT **("5" na stránce 170)**	MQZAO_PASS_ IDENTITY_CONTEXT	Nelze použít	Bez kontroly
KONTEXT MQOO_PASS_ALL_ **("5" na stránce 170, "6" na stránce 170)**	MQZAO_PASS _ALL_CONTEXT	Nelze použít	Bez kontroly
MQOO_SET_ IDENTITY_CONTEXT **("5" na stránce 170, "6" na stránce 170)**	MQZAO_SET_ IDENTITY_CONTEXT	Nelze použít	MQZAO_SET_ IDENTITY_CONTEXT **("7" na stránce 170)**
MQOO_SET_ ALL_CONTEXT **("5" na stránce 170, "8" na stránce 170)**	MQZAO_SET_ ALL_CONTEXT	Nelze použít	MQZAO_SET_ ALL_CONTEXT **("7" na stránce 170)**
MQOO_OUTPUT (přenosová fronta) **("9" na stránce 170)**	MQZAO_SET_ ALL_CONTEXT	Nelze použít	MQZAO_SET_ ALL_CONTEXT **("7" na stránce 170)**
MQOO_SET	MQZAO_SET	Nelze použít	Bez kontroly

Tabulka 20. Bezpečnostní autorizace potřebná pro volání MQOPEN (pokračování)			
Autorizace vyžadovaná pro:	**Objekt fronty ("1" na stránce 169)**	**Objekt procesu**	**Objekt správce front**
OPRÁVNĚNÍ UŽIVATELE MQOO_ALTERNATE_	**("10" na stránce 170)**	**("10" na stránce 170)**	MQZAO_ALTERNATE_ USER_AUTHORITY **("10" na stránce 170, "11" na stránce 170)**

Tabulka 21. Bezpečnostní autorizace potřebná pro volání MQPUT1			
Autorizace vyžadovaná pro:	**Objekt fronty ("1" na stránce 169)**	**Objekt procesu**	**Objekt správce front**
MQPMO_PASS_ IDENTITY_CONTEXT	MQZAO_PASS_ IDENTITY_CONTEXT **("12" na stránce 170)**	Nelze použít	Bez kontroly
MQPMO_PASS_ALL _CONTEXT	MQZAO_PASS_ ALL_CONTEXT **("12" na stránce 170)**	Nelze použít	Bez kontroly
MQPMO_SET_ IDENTITY_CONTEXT	MQZAO_SET_ IDENTITY_CONTEXT **("12" na stránce 170)**	Nelze použít	MQZAO_SET_ IDENTITY_CONTEXT **("7" na stránce 170)**
MQPMO_SET_ ALL_CONTEXT	MQZAO_SET_ ALL_CONTEXT **("12" na stránce 170)**	Nelze použít	MQZAO_SET_ ALL_CONTEXT **("7" na stránce 170)**
(Přenosová fronta) **("9" na stránce 170)**	MQZAO_SET_ ALL_CONTEXT	Nelze použít	MQZAO_SET_ ALL_CONTEXT **("7" na stránce 170)**
OPRÁVNĚNÍ UŽIVATELE MQPMO_ALTERNATE_	**("13" na stránce 170)**	Nelze použít	MQZAO_ALTERNATE_ USER_AUTHORITY **("11" na stránce 170)**

Tabulka 22. Bezpečnostní autorizace potřebná pro volání MQCLOSE			
Autorizace vyžadovaná pro:	**Objekt fronty ("1" na stránce 169)**	**Objekt procesu**	**Objekt správce front**
MQCO_DELETE	MQZAO_DELETE **("14" na stránce 170)**	Nelze použít	Nelze použít
MQCO_DELETE _PURGE	MQZAO_DELETE **("14" na stránce 170)**	Nelze použít	Nelze použít

Poznámky k tabulkám:

1. Pokud se otevírá modelová fronta:
   - Pro modelovou frontu je kromě oprávnění k otevření modelové fronty pro typ přístupu, pro který otevíráte, zapotřebí oprávnění MQZAO_DISPLAY.
   - K vytvoření dynamické fronty není zapotřebí oprávnění MQZAO_CREATE.
   - Identifikátoru uživatele použitému k otevření modelové fronty jsou automaticky udělena všechna oprávnění specifická pro danou frontu (ekvivalent k MQZAO_ALL) pro vytvořenou dynamickou frontu.

2. V závislosti na typu otevíraného objektu je kontrolována buď fronta, proces, seznam názvů, nebo objekt správce front.
3. Musí být zadána také hodnota MQOO_INPUT_ *. Tato volba je platná pro lokální, modelovou nebo alias frontu.
4. Tato kontrola se provádí pro všechny výstupní případy s výjimkou případu uvedeného v poznámce “9” na stránce 170.
5. Musí být uveden také parametr MQOO_OUTPUT.
6. MQOO_PASS_IDENTITY_CONTEXT je také odvozen z této volby.
7. Toto oprávnění je vyžadováno pro objekt správce front i pro konkrétní frontu.
8. MQOO_PASS_IDENTITY_CONTEXT, MQOO_PASS_ALL_CONTEXT a MQOO_SET_IDENTITY_CONTEXT jsou také odvozeny z této volby.
9. Tato kontrola se provádí pro lokální nebo modelovou frontu, která má atribut fronty *Usage* MQUS_TRANSMISSION, a otevírá se přímo pro výstup. Nepoužije se, pokud se otevírá vzdálená fronta (buď zadáním názvů vzdáleného správce front a vzdálené fronty, nebo zadáním názvu lokální definice vzdálené fronty).
10. Musí být zadán také alespoň jeden typ MQOOO_INQUIRE (pro libovolný typ objektu) nebo (pro fronty) MQOO_BROWSE, MQOO_INPUT_ *, MQOO_OUTPUT nebo MQOO_SET. Prováděná kontrola je stejná jako u ostatních zadaných voleb s použitím dodaného alternativního identifikátoru uživatele pro specifické oprávnění k objektu a aktuálního oprávnění aplikace pro kontrolu MQZAO_ALTERNATE_USER_IDENTIFIER.
11. Tato autorizace umožňuje zadat libovolné *AlternateUserId* .
12. Kontrola MQZAO_OUTPUT se provádí také v případě, že fronta nemá atribut fronty *Usage* s hodnotou MQUS_TRANSMISSION.
13. Prováděná kontrola je stejně jako u ostatních zadaných voleb, s použitím dodaného alternativního identifikátoru uživatele pro uvedené oprávnění fronty a aktuálního oprávnění aplikace pro kontrolu MQZAO_ALTERNATE_USER_IDENTIFIER.
14. Kontrola se provádí pouze v případě, že jsou pravdivá obě následující tvrzení:
    - Probíhá zavírání a odstraňování trvalé dynamické fronty.
    - Fronta nebyla vytvořena objektem MQOPEN, který vrátil používaný manipulátor objektu.

    V opačném případě není žádná kontrola.

Obecné poznámky:

1. Speciální autorizace MQZAO_ALL_MQI zahrnuje všechny následující autorizace, které jsou relevantní pro daný typ objektu:
   - MQZAO_CONNECT
   - MQZAO_INQUIRE
   - MQZAO_SET
   - MQZAO_BROWSE
   - MQZAO_INPUT
   - MQZAO_OUTPUT
   - MQZAO_PASS_IDENTITY_CONTEXT
   - MQZAO_PASS_ALL_CONTEXT
   - MQZAO_SET_IDENTITY_CONTEXT
   - MQZAO_SET_ALL_CONTEXT
   - OPRÁVNĚNÍ uživatele MQZAO_ALTERNATE_USER_AUTHORITY
2. MQZAO_DELETE (viz poznámka “14” na stránce 170) a MQZAO_DISPLAY jsou klasifikovány jako administrativní autorizace. Nejsou proto zahrnuty do MQZAO_ALL_MQI.
3. *Bez kontroly* znamená, že se neprovádí žádná kontrola autorizace.

4. *Nelze použít* znamená, že kontrola autorizace není pro tuto operaci relevantní. Nemůžete například zadat volání MQPUT do objektu procesu.

IBM i *Autorizace pro příkazy MQSC v řídicích PCF na systému IBM i*

Tato oprávnění umožňují uživateli vydávat příkazy administrace jako únikovou zprávu PCF. Tyto metody umožňují programu odeslat administrační příkaz jako zprávu správci front k provedení jménem tohoto uživatele.

Tento oddíl shrnuje autorizace potřebné pro každý příkaz MQSC obsažený v příkazu Escape PCF.

Nelze použít znamená, že kontrola autorizace není pro tuto operaci relevantní.

ID uživatele, pod kterým je spuštěn program, který zadává příkaz, musí mít také následující oprávnění:

- Oprávnění MQZAO_CONNECT ke správci front
- Oprávnění DISPLAY pro správce front, aby bylo možné provádět příkazy PCF.
- Oprávnění k zadání příkazů MQSC v textu příkazu Escape PCF

ALTER *objekt*

Objekt	**Je vyžadována autorizace**
Fronta	MQZAO_CHANGE
Téma	MQZAO_CHANGE
Proces	MQZAO_CHANGE
Správce front	MQZAO_CHANGE
Seznam názvů	MQZAO_CHANGE
Ověřovací informace	MQZAO_CHANGE
Kanál	MQZAO_CHANGE
Kanál připojení klienta	MQZAO_CHANGE
Modul listener	MQZAO_CHANGE
Služba	MQZAO_CHANGE

CLEAR *objekt*

Objekt	**Je vyžadována autorizace**
Fronta	MQZAO_CLEAR
Téma	MQZAO_CLEAR
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít
Ověřovací informace	Nelze použít
Kanál	Nelze použít
Kanál připojení klienta	Nelze použít
Modul listener	Nelze použít
Služba	Nelze použít

DEFINE *objekt* NOREPLACE (“1” na stránce 175)

Objekt	Je vyžadována autorizace
Fronta	MQZAO_CREATE **(“2” na stránce 175)**
Téma	MQZAO_CREATE **(“2” na stránce 175)**
Proces	MQZAO_CREATE **(“2” na stránce 175)**
Správce front	Nelze použít
Seznam názvů	MQZAO_CREATE **(“2” na stránce 175)**
Ověřovací informace	MQZAO_CREATE **(“2” na stránce 175)**
Kanál	MQZAO_CREATE **(“2” na stránce 175)**
Kanál připojení klienta	MQZAO_CREATE **(“2” na stránce 175)**
Modul listener	MQZAO_CREATE **(“2” na stránce 175)**
Služba	MQZAO_CREATE **(“2” na stránce 175)**

DEFINE *objekt* REPLACE (“1” na stránce 175, “3” na stránce 175)

Objekt	Je vyžadována autorizace
Fronta	MQZAO_CHANGE
Téma	MQZAO_CHANGE
Proces	MQZAO_CHANGE
Správce front	Nelze použít
Seznam názvů	MQZAO_CHANGE
Ověřovací informace	MQZAO_CHANGE
Kanál	MQZAO_CHANGE
Kanál připojení klienta	MQZAO_CHANGE
Modul listener	MQZAO_CHANGE
Služba	MQZAO_CHANGE

DELETE *objekt*

Objekt	Je vyžadována autorizace
Fronta	MQZAO_DELETE
Téma	MQZAO_DELETE
Proces	MQZAO_DELETE
Správce front	Nelze použít
Seznam názvů	MQZAO_DELETE
Ověřovací informace	MQZAO_DELETE
Kanál	MQZAO_DELETE
Kanál připojení klienta	MQZAO_DELETE
Modul listener	MQZAO_DELETE

Objekt	Je vyžadována autorizace
Služba	MQZAO_DELETE

DISPLAY *objekt*

Objekt	Je vyžadována autorizace
Fronta	MQZAO_DISPLAY
Téma	MQZAO_DISPLAY
Proces	MQZAO_DISPLAY
Správce front	MQZAO_DISPLAY
Seznam názvů	MQZAO_DISPLAY
Ověřovací informace	MQZAO_DISPLAY
Kanál	MQZAO_DISPLAY
Kanál připojení klienta	MQZAO_DISPLAY
Modul listener	
Služba	

Odeslat signál Ping pro kanál

Objekt	Je vyžadována autorizace
Fronta	Nelze použít
Téma	Nelze použít
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít
Ověřovací informace	Nelze použít
Kanál	MQZAO_CONTROL
Kanál připojení klienta	Nelze použít
Modul listener	Nelze použít
Služba	Nelze použít

Resetovat kanál

Objekt	Je vyžadována autorizace
Fronta	Nelze použít
Téma	Nelze použít
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít
Ověřovací informace	Nelze použít
Kanál	MQZAO_CONTROL_EXTENDED

Objekt	Je vyžadována autorizace
Kanál připojení klienta	Nelze použít
Modul listener	Nelze použít
Služba	Nelze použít

Vyřešit kanál

Objekt	Je vyžadována autorizace
Fronta	Nelze použít
Téma	Nelze použít
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít
Ověřovací informace	Nelze použít
Kanál	MQZAO_CONTROL_EXTENDED
Kanál připojení klienta	Nelze použít
Modul listener	Nelze použít
Služba	Nelze použít

START *objekt*

Objekt	Je vyžadována autorizace
Fronta	Nelze použít
Téma	Nelze použít
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít
Ověřovací informace	Nelze použít
Kanál	MQZAO_CONTROL
Kanál připojení klienta	Nelze použít
Modul listener	MQZAO_CONTROL
Služba	MQZAO_CONTROL

STOP *objekt*

Objekt	Je vyžadována autorizace
Fronta	Nelze použít
Téma	Nelze použít
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít

Objekt	Je vyžadována autorizace
Ověřovací informace	Nelze použít
Kanál	MQZAO_CONTROL
Kanál připojení klienta	Nelze použít
Modul listener	MQZAO_CONTROL
Služba	MQZAO_CONTROL

Poznámka:

1. Pro příkazy DEFINE je oprávnění MQZAO_DISPLAY vyžadováno také pro objekt LIKE, pokud je zadán, nebo pro příslušný SYSTEM.DEFAULT.xxx , pokud je operátor LIKE vynechán.
2. Oprávnění MQZAO_CREATE není specifické pro konkrétní objekt nebo typ objektu. Oprávnění k vytvoření je uděleno pro všechny objekty pro uvedeného správce front zadáním typu objektu QMGR v příkazu GRTMQMAUT .
3. Tato volba se použije, pokud objekt, který má být nahrazen, již existuje. Pokud tomu tak není, kontrola je jako u DEFINE *object* NOREPLACE.

IBM i *Autorizace pro příkazy PCF na systému IBM i*

Tato oprávnění umožňují uživateli vydávat příkazy administrace jako příkazy PCF. Tyto metody umožňují programu odeslat administrační příkaz jako zprávu správci front k provedení jménem tohoto uživatele.

Tento oddíl shrnuje autorizace potřebné pro každý příkaz PCF.

Bez kontroly znamená, že se neprovádí žádná kontrola autorizace. *Nelze použít* znamená, že kontrola autorizace není pro tuto operaci relevantní.

ID uživatele, pod kterým je spuštěn program, který zadává příkaz, musí mít také následující oprávnění:

- Oprávnění MQZAO_CONNECT ke správci front
- Oprávnění DISPLAY pro správce front, aby bylo možné provádět příkazy PCF.

Speciální autorizace MQZAO_ALL_ADMIN zahrnuje následující oprávnění:

- MQZAO_CHANGE
- MQZAO_CLEAR
- MQZAO_DELETE
- MQZAO_DISPLAY
- MQZAO_CONTROL
- MQZAO_CONTROL_EXTENDED

Příkaz MQZAO_CREATE není zahrnut, protože není specifický pro konkrétní objekt nebo typ objektu.

Změnit *objekt*

Objekt	Je vyžadována autorizace
Fronta	MQZAO_CHANGE
Téma	MQZAO_CHANGE
Proces	MQZAO_CHANGE
Správce front	MQZAO_CHANGE
Seznam názvů	MQZAO_CHANGE
Ověřovací informace	MQZAO_CHANGE
Kanál	MQZAO_CHANGE

Objekt	Je vyžadována autorizace
Kanál připojení klienta	MQZAO_CHANGE
Modul listener	MQZAO_CHANGE
Služba	MQZAO_CHANGE

Vymazat *objekt*

Objekt	Je vyžadována autorizace
Fronta	MQZAO_CLEAR
Téma	MQZAO_CLEAR
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít
Ověřovací informace	Nelze použít
Kanál	Nelze použít
Kanál připojení klienta	Nelze použít
Modul listener	Nelze použít
Služba	Nelze použít

Kopírovat *objekt* (bez náhrady) (“1” na stránce 181)

Objekt	Je vyžadována autorizace
Fronta	MQZAO_CREATE **(“2” na stránce 181)**
Téma	MQZAO_CREATE **(“2” na stránce 181)**
Proces	MQZAO_CREATE **(“2” na stránce 181)**
Správce front	Nelze použít
NamelistMQZAO_CREATE	MQZAO_CREATE **(“2” na stránce 181)**
Ověřovací informace	MQZAO_CREATE **(“2” na stránce 181)**
Kanál	MQZAO_CREATE **(“2” na stránce 181)**
Kanál připojení klienta	MQZAO_CREATE **(“2” na stránce 181)**
Modul listener	MQZAO_CREATE **(“2” na stránce 181)**
Služba	MQZAO_CREATE **(“2” na stránce 181)**

Kopírovat *objekt* (s nahrazením) (“1” na stránce 181, “4” na stránce 181)

Objekt	Je vyžadována autorizace
Fronta	MQZAO_CHANGE
Téma	MQZAO_CHANGE
Proces	MQZAO_CHANGE
Správce front	Nelze použít
Seznam názvů	MQZAO_CHANGE

Objekt	Je vyžadována autorizace
Ověřovací informace	MQZAO_CHANGE
Kanál	MQZAO_CHANGE
Kanál připojení klienta	MQZAO_CHANGE
Modul listener	MQZAO_CHANGE
Služba	MQZAO_CHANGE

Vytvořit *objekt* (bez náhrady) (“3” na stránce 181)

Objekt	Je vyžadována autorizace
Fronta	MQZAO_CREATE **(“2” na stránce 181)**
Téma	MQZAO_CREATE **(“2” na stránce 181)**
Proces	MQZAO_CREATE **(“2” na stránce 181)**
Správce front	Nelze použít
Seznam názvů	MQZAO_CREATE **(“2” na stránce 181)**
Ověřovací informace	MQZAO_CREATE **(“2” na stránce 181)**
Kanál	MQZAO_CREATE **(“2” na stránce 181)**
Kanál připojení klienta	MQZAO_CREATE **(“2” na stránce 181)**
Modul listener	MQZAO_CHANGE
Služba	MQZAO_CHANGE

Vytvořit *objekt* (s nahrazením) (“3” na stránce 181, “4” na stránce 181)

Objekt	Je vyžadována autorizace
Fronta	MQZAO_CHANGE
Téma	MQZAO_CHANGE
Proces	MQZAO_CHANGE
Správce front	Nelze použít
Seznam názvů	MQZAO_CHANGE
Ověřovací informace	MQZAO_CHANGE
Kanál	MQZAO_CHANGE
Kanál připojení klienta	MQZAO_CHANGE
Modul listener	MQZAO_CHANGE
Služba	MQZAO_CHANGE

Odstranit *objekt*

Objekt	Je vyžadována autorizace
Fronta	MQZAO_DELETE
Téma	MQZAO_DELETE
Proces	MQZAO_DELETE

Objekt	Je vyžadována autorizace
Správce front	MQZAO_DELETE
Seznam názvů	MQZAO_DELETE
Ověřovací informace	MQZAO_DELETE
Kanál	MQZAO_DELETE
Kanál připojení klienta	MQZAO_DELETE
Modul listener	MQZAO_DELETE
Služba	MQZAO_DELETE

Dotaz na *objekt*

Objekt	Je vyžadována autorizace
Fronta	MQZAO_DISPLAY
Téma	MQZAO_DISPLAY
Proces	MQZAO_DISPLAY
Správce front	MQZAO_DISPLAY
Seznam názvů	MQZAO_DISPLAY
Ověřovací informace	MQZAO_DISPLAY
Kanál	MQZAO_DISPLAY
Kanál připojení klienta	MQZAO_DISPLAY
Modul listener	MQZAO_DISPLAY
Služba	MQZAO_DISPLAY

Zjistit názvy *objektů*

Objekt	Je vyžadována autorizace
Fronta	Bez kontroly
Téma	Bez kontroly
Proces	Bez kontroly
Správce front	Bez kontroly
Seznam názvů	Bez kontroly
Ověřovací informace	Bez kontroly
Kanál	Bez kontroly
Kanál připojení klienta	Bez kontroly
Modul listener	Bez kontroly
Služba	Bez kontroly

Odeslat signál Ping pro kanál

Objekt	Je vyžadována autorizace
Fronta	Nelze použít

Objekt	Je vyžadována autorizace
Téma	Nelze použít
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít
Ověřovací informace	Nelze použít
Kanál	MQZAO_CONTROL
Kanál připojení klienta	Nelze použít
Modul listener	Nelze použít
Služba	Nelze použít

Resetovat kanál

Objekt	Je vyžadována autorizace
Fronta	Nelze použít
Téma	Nelze použít
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít
Ověřovací informace	Nelze použít
Kanál	MQZAO_CONTROL_EXTENDED
Kanál připojení klienta	Nelze použít
Modul listener	Nelze použít
Služba	Nelze použít

Obnovit statistiku front

Objekt	Je vyžadována autorizace
Fronta	MQZAO_DISPLAY a MQZAO_CHANGE
Téma	Nelze použít
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít
Ověřovací informace	Nelze použít
Kanál	Nelze použít
Kanál připojení klienta	Nelze použít
Modul listener	
Služba	

Vyřešit kanál

Objekt	Je vyžadována autorizace
Fronta	Nelze použít
Téma	Nelze použít
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít
Ověřovací informace	Nelze použít
Kanál	MQZAO_CONTROL_EXTENDED
Kanál připojení klienta	Nelze použít
Modul listener	Nelze použít
Služba	Nelze použít

Spustit kanál

Objekt	Je vyžadována autorizace
Fronta	Nelze použít
Téma	Nelze použít
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít
Ověřovací informace	Nelze použít
Kanál	MQZAO_CONTROL
Kanál připojení klienta	Nelze použít
Modul listener	Nelze použít
Služba	Nelze použít

Ukončit kanál

Objekt	Je vyžadována autorizace
Fronta	Nelze použít
Téma	Nelze použít
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít
Ověřovací informace	Nelze použít
Kanál	MQZAO_CONTROL
Kanál připojení klienta	Nelze použít
Modul listener	Nelze použít

Objekt	Je vyžadována autorizace
Služba	Nelze použít

Poznámka:

1. Pro příkazy Copy je oprávnění MQZAO_DISPLAY také potřebné pro objekt From.
2. Oprávnění MQZAO_CREATE není specifické pro konkrétní objekt nebo typ objektu. Oprávnění k vytvoření je uděleno pro všechny objekty pro uvedeného správce front zadáním typu objektu QMGR v příkazu GRTMQMAUT .
3. Pro příkazy Create je také vyžadováno oprávnění MQZAO_DISPLAY pro příslušný systém SYSTEM.DEFAULT.* objekt.
4. Tato volba se použije, pokud objekt, který má být nahrazen, již existuje. Pokud tomu tak není, je kontrola stejně jako pro Kopírovat nebo Vytvořit bez náhrady.

IBM i Generické profily OAM na systému IBM i

Generické profily správce oprávnění k objektu (OAM) vám umožňují nastavit oprávnění, které má uživatel, na mnoho objektů najednou, místo abyste museli vydávat samostatné příkazy **GRTMQMAUT** pro každý jednotlivý objekt, když je vytvořen. Použití generických profilů v příkazu **GRTMQMAUT** vám umožňuje nastavit generické oprávnění pro všechny budoucí objekty vytvořené tak, aby vyhovovaly tomuto profilu.

Zbytek tohoto oddílu podrobněji popisuje použití generických profilů:

- "Použití zástupných znaků" na stránce 181
- "Priority profilu" na stránce 182

Použití zástupných znaků

Profil je generický použitím speciálních znaků (zástupných znaků) v názvu profilu. Zástupný znak otazník (?) například odpovídá libovolnému jednotlivému znaku v názvu. Pokud tedy zadáte hodnotu ABC.?EF, bude autorizace, kterou udělíte tomuto profilu, platit pro všechny objekty vytvořené s názvy ABC.DEF, ABC.CEF, ABC.BEFatd.

K dispozici jsou následující zástupné znaky:

?

Otazník (?) zastupuje libovolný jeden znak. Například AB.?D by se použilo na objekty AB.CD, AB.EDa AB.FD.

*****

Použijte hvězdičku (*) jako:

- *Kvalifikátor* v názvu profilu tak, aby odpovídal libovolnému kvalifikátoru v názvu objektu. Kvalifikátor je část názvu objektu oddělená tečkou. Název objektu ABC.DEF.GHI se například skládá z kvalifikátorů ABC, DEF a GHI.

  Například ABC.*.JKL by se použilo na objekty ABC.DEF.JKLa ABC.GHI.JKL. (Všimněte si, že se **nebude** vztahovat na ABC.JKL ; * použité v tomto kontextu vždy označuje jeden kvalifikátor.)
- Znak v kvalifikátoru v názvu profilu, který odpovídá žádnému nebo více znakům v kvalifikátoru v názvu objektu.

  Například ABC.DE*.JKL by se použilo na objekty ABC.DE.JKL, ABC.DEF.JKLa ABC.DEGH.JKL.

******

Dvojitou hvězdičku (**) ***jednou*** použijte v názvu profilu jako:

- Celý název profilu, který má odpovídat všem názvům objektů. Pokud například použijete klíčové slovo OBJTYPE (*PRC) k identifikaci procesů, použijte ** jako název profilu, změníte oprávnění pro všechny procesy.

- Jako počáteční, střední nebo koncový kvalifikátor v názvu profilu odpovídá žádnému nebo více kvalifikátorům v názvu objektu. Například `**.ABC` identifikuje všechny objekty s konečným kvalifikátorem ABC.

Priority profilu

Důležitým bodem, který je třeba pochopit při používání generických profilů, je priorita, kterou mají profily při rozhodování o tom, která oprávnění se mají použít na vytvářený objekt. Předpokládejme například, že jste zadali příkazy:

```
GRTMQMAUT OBJ(AB.*) OBJTYPE(*Q) USER(FRED) AUT(*PUT) MQMNAME(MYQMGR)
GRTMQMAUT OBJ(AB.C*) OBJTYPE(*Q) USER(FRED) AUT(*GET) MQMNAME(MYQMGR)
```

První poskytuje oprávnění vložení ke všem frontám pro činitele FRED s názvy, které odpovídají profilu AB.*; druhý poskytuje oprávnění k získání pro stejné typy front, které odpovídají profilu AB.C*.

Předpokládejme, že nyní vytvoříte frontu s názvem AB.CD. Podle pravidel pro porovnávání se zástupnými znaky se na tuto frontu může vztahovat buď GRTMQMAUT, nebo GRTMQMAUT. Tak, má to dát, nebo získat autoritu?

Chcete-li najít odpověď, použijte pravidlo, které vždy, když lze na objekt použít více profilů, **použije se pouze nejspecifičtější**. Toto pravidlo použijete tak, že porovnáte názvy profilů zleva doprava. Kdekoli se liší, negenerický znak je specifičtější než generický znak. Takže v předchozím příkladu se jedná o frontu AB.CD má oprávnění **získat** (AB.C* je specifičtější než AB. *).

Při porovnávání generických znaků je pořadí *specifičnosti* následující:

1. ?
2. *
3. **

IBM i Určení nainstalované autorizační služby v systému IBM i

Můžete určit, která komponenta služby autorizace se má použít.

Parametr **Service Component name** na systému **GRTMQMAUT** a **RVKMQMAUT** vám umožňuje uvést název instalované komponenty služby autorizace.

Výběr **F24** na počátečním panelu, následovaný **F9=All parametry** na dalším panelu libovolného příkazu vám umožňuje uvést buď nainstalovanou komponentu autorizace (*DFT), nebo název požadované komponenty služby autorizace uvedené v sekci Služba souboru qm.ini správce front.

DSPMQMAUT má také tento další parametr. Tento parametr vám umožňuje prohledat všechny instalované komponenty autorizace (*DFT) nebo uvedený název komponenty služby autorizace pro uvedený název objektu, typ objektu a uživatele

IBM i Práce s profily oprávnění a bez nich na systému IBM i

Pomocí těchto informací se dozvíte, jak pracovat s profily oprávnění a jak pracovat bez profilů oprávnění.

Můžete pracovat s profily oprávnění, jak je vysvětleno v části “Práce s profily oprávnění” na stránce 182, nebo bez nich, jak je vysvětleno zde:

Chcete-li pracovat bez profilů oprávnění, použijte *NONE jako parametr oprávnění na systému **GRTMQMAUT** k vytvoření profilů bez oprávnění. To ponechá všechny existující profily beze změny.

V systému **RVKMQMAUT**použijte *REMOVE jako parametr Oprávnění k odebrání existujícího profilu oprávnění.

Práce s profily oprávnění

K profilování oprávnění jsou přidruženy dva příkazy:

- **WRKMQMAUT**
- **WRKMQMAUTD**

K těmto příkazům můžete přistupovat přímo z příkazového řádku nebo z panelu WRKMQM pomocí:

1. Zadáním názvu správce front a stisknutím klávesy `Enter` získáte přístup k panelu výsledků produktu **WRKMQM** .
2. Výběr `F23=More options` na tomto panelu.

Volba 24 vybere panel výsledků pro **WRKMQMAUT** příkaz a volba 25 vybere příkaz **WRKMQMAUTI** , který se používá s vrstvou vazeb SSL.

WRKMQMAUT

Tento příkaz vám umožňuje pracovat s daty oprávnění zadrženými ve frontě oprávnění.

Poznámka: Chcete-li spustit tento příkaz, musíte mít oprávnění `*connect` a `*admdsp` ke správci front. Chcete-li však vytvořit nebo odstranit profil, potřebujete oprávnění QMQMADM.

Pokud vypisujete informace na obrazovku, zobrazí se seznam názvů profilů oprávnění spolu s jejich typy. Pokud vytisknete výstup, obdržíte podrobný seznam všech dat oprávnění, registrovaných uživatelů a jejich oprávnění.

Zadáním názvu objektu nebo profilu na tomto panelu a stisknutím klávesy ENTER se dostanete na panel výsledků pro produkt **WRKMQMAUT** .

Vyberete-li volbu `4=Delete`, přejdete na nový panel, ze kterého můžete potvrdit, že chcete odstranit všechna jména uživatelů registrovaná pro zadaný generický název profilu oprávnění. Tato volba spustí **RVKMQMAUT** s volbou *REMOVE pro všechny uživatele a použije **pouze** na generické názvy profilů.

Vyberete-li volbu `12=Work with profile` , přejdete na panel výsledků příkazu **WRKMQMAUTD** , jak je vysvětleno v tématu “WRKMQMAUTD” na stránce 183.

WRKMQMAUTD

Tento příkaz vám umožňuje zobrazit všechny uživatele registrované s konkrétním názvem profilu oprávnění a typem objektu. Chcete-li spustit tento příkaz, musíte mít oprávnění `*connect` a `*admdsp` ke správci front. Chcete-li však udělit, spustit, vytvořit nebo odstranit profil, potřebujete oprávnění QMQMADM.

Výběrem volby `F24=More keys` z počátečního vstupního panelu následované volbou `F9=All Parameters` zobrazíte název komponenty služby jako pro **GRTMQMAUT** a **RVKMQMAUT**.

Poznámka: Klíč `F11=Display Object Authorizations` přepíná mezi následujícími typy oprávnění:

- Autorizace objektů
- Autorizace kontextu
- Autorizace MQI

Volby na obrazovce jsou:

2=Grant
Přenese vás na panel **GRTMQMAUT** , abyste přidali aktuální oprávnění.

3=Revoke
Přenese vás na panel **RVKMQMAUT** , abyste odebrali některé z aktuálních definic

4=Delete
Přenese vás na panel, který vám umožňuje odstranit data oprávnění pro uvedené uživatele. Spustí se **RVKMQMAUT** s volbou *REMOVE.

5=Display
Přenese vás na existující příkaz **DSPMQMAUT** .

F6=Create
Přenese vás na panel **GRTMQMAUT** , který vám umožňuje vytvořit záznam oprávnění k profilu.

IBM i Pokyny pro správce oprávnění k objektu na systému IBM i

Další pokyny a tipy pro použití správce OAM (Object Authority Manager)

Omezit přístup k citlivým operacím

Některé operace jsou citlivé; omezte je na oprávněné uživatele. Například:

- Přístup k některým speciálním frontám, jako jsou přenosové fronty nebo fronta příkazů `SYSTEM.ADMIN.COMMAND.QUEUE`
- Spuštění programů, které používají úplné volby kontextu MQI
- Vytváření a kopírování front aplikací

Adresáře správce front

Adresáře a knihovny obsahující fronty a další data správce front jsou pro produkt soukromé. Nepoužívejte standardní příkazy operačního systému k udělení nebo zrušení oprávnění k prostředkům MQI.

Fronty

Oprávnění k dynamické frontě je založeno na modelové frontě, ze které je odvozena, ale nemusí být nutně stejné.

V případě front aliasů a vzdálených front se jedná o autorizaci objektu samotného, nikoli o frontu, na kterou se alias nebo vzdálená fronta interpretuje. Je možné autorizovat profil uživatele pro přístup k alias frontě, která se interpretuje jako lokální fronta, ke které nemá profil uživatele přístupová oprávnění.

Omezte oprávnění k vytváření front na oprávněné uživatele. Pokud tak neučiníte, uživatelé mohou obejít běžné řízení přístupu vytvořením aliasu.

Oprávnění alternativního uživatele

Oprávnění alternativního uživatele řídí, zda může jeden profil uživatele použít oprávnění jiného profilu uživatele při přístupu k objektu IBM MQ . Tato technika je nezbytná v případech, kdy server přijímá požadavky od programu a server chce zajistit, aby program měl požadované oprávnění k požadavku. Server může mít požadované oprávnění, ale musí vědět, zda má program oprávnění pro akce, které požadoval.

Příklad:

- Program serveru spuštěný pod profilem uživatele PAYSERV načte zprávu požadavku z fronty, která byla vložena do fronty profilem uživatele USER1.
- Když program serveru obdrží zprávu požadavku, zpracuje požadavek a vloží odpověď zpět do fronty pro odpověď uvedené se zprávou požadavku.
- Místo použití vlastního profilu uživatele (PAYSERV) k autorizaci otevření fronty pro odpověď může server uvést jiný profil uživatele, v tomto případě USER1. V tomto příkladu můžete použít oprávnění alternativního uživatele k řízení, zda je PAYSERV oprávněn uvést USER1 jako alternativní profil uživatele, když otevře frontu pro odpověď.

Profil alternativního uživatele je uveden v poli *`AlternateUserId`* deskriptoru objektu.

Poznámka: Můžete použít alternativní profily uživatele na libovolném objektu IBM MQ . Použití profilu alternativního uživatele nemá vliv na profil uživatele používaný jinými správci prostředků.

Oprávnění kontextu

Kontext je informace, která se týká konkrétní zprávy a je obsažena v deskriptoru zprávy MQMD, který je součástí zprávy.

Popisy polí deskriptoru zpráv souvisejících s kontextem viz MQMD-deskriptor zpráv.

Informace o volbách kontextu viz Kontext zprávy.

Aspekty vzdáleného zabezpečení

Pro vzdálené zabezpečení zvažte:

Oprávnění pro operaci vložení (Put)
Pro zabezpečení v rámci správců front můžete určit oprávnění vložení, které bude použito v případě, že kanál obdrží zprávu odeslanou od jiného správce front.

Tento parametr je platný pouze pro typy kanálů RCVR, RQSTR nebo CLUSRCVR. Následujícím způsobem zadejte atribut kanálu PUTAUT:

DEF
Výchozí profil uživatele. Jedná se o profil uživatele QMQM, pod kterým je spuštěn agent kanálu zpráv.

CTX
Profil uživatele v kontextu zprávy.

Přenosové fronty
Správci front automaticky vkládají vzdálené zprávy do přenosové fronty; není vyžadováno žádné speciální oprávnění. Vložení zprávy přímo do přenosové fronty však vyžaduje speciální oprávnění.

Uživatelské procedury kanálu
Pro zvýšení zabezpečení lze použít uživatelské procedury kanálu.

Záznamy ověření kanálu
Slouží k přesnějšímu řízení přístupu k připojovacím systémům na úrovni kanálu.

Další informace o vzdáleném zabezpečení viz “Autorizace kanálu” na stránce 113.

Ochrana kanálů pomocí SSL/TLS

Protokol TLS (Transport Layer Security) poskytuje zabezpečení kanálu s ochranou proti odposlechu, manipulaci a zosobnění. Podpora produktu IBM MQ pro protokol TLS umožňuje určit v definici kanálu, že konkrétní kanál používá zabezpečení TLS. Můžete také určit podrobnosti požadovaného zabezpečení, například šifrovací algoritmus, který chcete použít.

Podpora TLS v produktu IBM MQ používá *objekt ověřovacích informací* správce front a různé příkazy CL a MQSC a parametry správce front a kanálu, které definují podporu TLS vyžadovanou podrobně.

Následující příkazy CL podporují TLS:

WRKMQMAUTI
Práce s atributy objektu ověřovacích informací.

CHGMQMAUTI
Upravte atributy objektu ověřovacích informací.

CRTMQMAUTI
Vytvořte objekt ověřovacích informací.

CPYMQMAUTI
Vytvořte objekt ověřovacích informací zkopírováním existujícího objektu.

DLTMQMAUTI
Odstranit objekt ověřovacích informací.

DSPMQMAUTI
Zobrazí atributy pro specifický objekt ověřovacích informací.

Přehled zabezpečení kanálu pomocí protokolu TLS naleznete v tématu

- Ochrana kanálů pomocí protokolu TLS

Podrobnosti o příkazech PCF přidružených k protokolu TLS naleznete v tématu

- Změnit, kopírovat a vytvořit objekt ověřovacích informací
- Odstranit objekt ověřovacích informací
- Zjistit objekt ověřovacích informací

z/OS Nastavení zabezpečení na systému z/OS

Aspekty zabezpečení specifické pro produkt z/OS.

Zabezpečení v produktu IBM MQ for z/OS je řízeno pomocí produktu RACF nebo ekvivalentního externího správce zabezpečení (ESM).

Následující pokyny předpokládají, že používáte RACF.

Související pojmy

Scénář zabezpečení: dva správci front v systému z/OS

Scénář zabezpečení: Skupina sdílení front v systému z/OS

z/OS Třídy zabezpečení RACF

Třídy RACF se používají k uchování profilů požadovaných pro kontrolu zabezpečení produktu IBM MQ . Mnoho členských tříd má ekvivalentní skupinové třídy. Musíte aktivovat třídy a povolit jim přijetí generických profilů.

Každá třída RACF obsahuje jeden nebo více profilů použitých v určitém bodě posloupnosti kontrol, jak ukazuje Tabulka 23 na stránce 186.

Tabulka 23. RACF tříd používaných IBM MQ

Třída člena	Třída skupiny	Obsah
MQADMIN	GMQADMIN	Profily, které se používají hlavně pro administrativní funkce. Příklad: • Profily pro přepínače zabezpečení IBM MQ . • Profil zabezpečení RESLEVEL. • Profily pro alternativní zabezpečení uživatele. • Profily pro zabezpečení kontextu. • Profily pro zabezpečení prostředků příkazu. Tato třída může obsahovat pouze profily RACF s velkými písmeny.
MXADMIN	GMXADMIN-počet uživatelů	Profily, které se používají hlavně pro administrativní funkce. Příklad: • Profily pro přepínače zabezpečení IBM MQ . • Profil zabezpečení RESLEVEL. • Profily pro alternativní zabezpečení uživatele. • Profily pro zabezpečení kontextu. • Profily pro zabezpečení prostředků příkazu. Tato třída může obsahovat profily RACF s velkými i smíšenými písmeny.

Tabulka 23. RACF tříd používaných IBM MQ (pokračování)		
Třída člena	**Třída skupiny**	**Obsah**
MQCONN		Profily používané pro zabezpečení připojení.
MQCMDS		Profily používané pro zabezpečení příkazů.
MQQUEUE	Fronta GMQQUEUE	Profily s velkými písmeny používané v zabezpečení prostředků fronty.
MXQUEUE	GMXQUEUE- zařazení do fronty	Profily s malými i velkými písmeny používané v zabezpečení prostředků fronty.
MQPROC	GMQPROC	Profily s velkými písmeny používané v zabezpečení prostředků procesu.
MXPROC	GMXPROC	Profily s malými i velkými písmeny používané v zabezpečení prostředků procesu.
MQNLIST	GMQNLIST	Profily s velkými písmeny používané v zabezpečení prostředků seznamu názvů.
MXNLIST	GMXNLIST	Profily s malými i velkými písmeny používané v zabezpečení prostředků seznamu názvů.
MXTOPIC	GMXTOPIC	Profily s malými i velkými písmeny používané v zabezpečení tématu.

Některé třídy mají související *třídu skupiny* , která vám umožňuje sestavit skupiny prostředků, které mají podobné požadavky na přístup. Podrobnosti o rozdílech mezi třídami členů a skupin a o tom, kdy použít třídu člena nebo skupiny, naleznete v příručce z/OS Security Server RACF Security Administrator's Guide.

Třídy musí být aktivovány před provedením kontrol zabezpečení. Chcete-li aktivovat všechny třídy IBM MQ , můžete použít tento příkaz RACF :

```
SETROPTS CLASSACT(MQADMIN,MXADMIN,MQQUEUE,MXQUEUE,MQPROC,MXPROC,
                  MQNLIST,MXNLIST,MXTOPIC,MQCONN,MQCMDS)
```

Měli byste se také ujistit, že jste nastavili třídy tak, aby mohly přijímat generické profily. To provedete také pomocí příkazu RACF **SETROPTS**, například:

```
SETROPTS GENERIC(MQADMIN,MXADMIN,MQQUEUE,MXQUEUE,MQPROC,MXPROC,
                 MQNLIST,MXNLIST,MXTOPIC,MQCONN,MQCMDS)
```

z/OS RACF profily

Všechny profily RACF používané produktem IBM MQ obsahují předponu, která je buď názvem správce front, nebo názvem skupiny sdílení front. Při použití znaku procenta jako zástupného znaku buďte opatrní.

Všechny profily systému RACF používané produktem IBM MQ obsahují předponu. V případě zabezpečení na úrovni skupiny sdílení front se jedná o název skupiny sdílení front. V případě zabezpečení na úrovni správce front je předponou název správce front. Pokud používáte kombinaci zabezpečení na úrovni správce front a skupiny sdílení front, budete používat profily s oběma typy předpon. Skupina sdílení front a zabezpečení na úrovni správce front jsou popsány v tématu Ovládací prvky a volby zabezpečení v produktu IBM MQ for z/OS.

Chcete-li například chránit frontu s názvem QUEUE_FOR_SUBSCRIBER_LIST ve skupině sdílení front QSG1 na úrovni skupiny sdílení front, bude příslušný profil definován pro RACF jako:

```
RDEFINE MQQUEUE QSG1.QUEUE_FOR_SUBSCRIBER_LIST
```

Chcete-li chránit frontu s názvem QUEUE_FOR_LOST_CARD_LIST, která patří ke správci front STCD na úrovni správce front, bude příslušný profil definován jako RACF :

```
RDEFINE MQQUEUE STCD.QUEUE_FOR_LOST_CARD_LIST
```

To znamená, že různí správci front a skupiny sdílení front mohou sdílet stejnou databázi RACF , a přesto mohou mít různé volby zabezpečení.

Nepoužívejte generické názvy správců front v profilech, abyste se vyhnuli neočekávanému přístupu uživatelů.

IBM MQ umožňuje použití znaku procenta (%) v názvech objektů. Produkt RACF však používá znak% jako zástupný znak pro jeden znak. To znamená, že když definujete název objektu se znakem% v názvu, musíte to zvážit při definování odpovídajícího profilu.

Například pro frontu CREDIT_CARD_ %_RATE_INQUIRY ve správci front CRDP bude profil definován jako RACF následujícím způsobem:

```
RDEFINE MQQUEUE CRDP.CREDIT_CARD_%_RATE_INQUIRY
```

Tuto frontu nelze chránit generickým profilem, například CRDP. * *.

Produkt IBM MQ umožňuje v názvech objektů používat malá a velká písmena. Tyto objekty můžete chránit definováním:

1. profily se smíšenými velkými a velkými písmeny v příslušných třídách RACF , nebo
2. Generické profily v odpovídajících velkých třídách RACF .

Chcete-li používat profily se smíšenými velkými a velkými písmeny a třídy RACF , musíte postupovat podle kroků popsaných v části “Migrace správce front z/OS na zabezpečení s různými případy” na stránce 268.

Existují některé profily nebo části profilů, které zůstávají pouze velkými písmeny, protože hodnoty jsou poskytovány produktem IBM MQ. Patří mezi ně:

- Přepnout profily.
- Všechny kvalifikátory vyšší úrovně (HLQ) včetně identifikátorů subsystému a skupin sdílení front.
- Profily pro objekty SYSTEM.
- Profily pro výchozí objekty.
- Třída **MQCMDS** , takže všechny profily příkazů jsou pouze velká písmena.
- Třída **MQCONN** , takže všechny profily připojení jsou pouze velká písmena.
- **RESLEVEL** profilů.
- Kvalifikace `'object'` v profilech prostředků příkazu; například `hlq.QUEUE.queuename`. Název prostředku má pouze malá a velká písmena.
- Profily dynamických front `hlq.CSQOREXX.*`, `hlq.CSQUTIL.*`a `CSQXCMD.*`.
- Část `'CONTEXT'` položky `hlq.CONTEXT.resourcename`.
- Část `'ALTERNATE.USER'` položky `hlq.ALTERNATE.USER.userid`.

Můžete například definovat profil pro udělení přístupu ke frontě s názvem `PAYROLL.Dept1` ve správci front `QM01` jedním z následujících způsobů.

- Používáte-li profily se smíšenými případy, můžete definovat profil ve třídě IBM MQ RACF MXQUEUE pomocí následujícího příkazu:

```
RDEFINE MXQUEUE MQ01.PAYROLL.Dept1
```

- Používáte-li profily s velkými písmeny, můžete definovat profil ve třídě IBM MQ RACF MQQUEUE pomocí následujícího příkazu:

```
RDEFINE MQQUEUE MQ01.PAYROLL.*
```

První příklad, používající profily smíšených případů, vám poskytuje podrobnější kontrolu nad udělením oprávnění pro přístup k prostředku.

z/OS Přepnout profily

Chcete-li řídit kontrolu zabezpečení prováděnou produktem IBM MQ, použijte *profily přepínače*. Profil přepínače je normální profil RACF , který má speciální význam pro IBM MQ. Seznam pro přístup v profilech přepínače není používán produktem IBM MQ.

Produkt IBM MQ udržuje interní přepínač pro každý typ přepínače zobrazený v tabulkách Profily přepínače pro zabezpečení na úrovni subsystému, Profily přepínače pro skupinu sdílení front nebo zabezpečení na úrovni správce fronta Profily přepínače pro kontrolu prostředků. Profily přepínače lze udržovat na úrovni skupiny sdílení front, na úrovni správce front nebo v kombinaci obojího. Pomocí jediné sady profilů přepínačů zabezpečení skupiny sdílení front můžete řídit zabezpečení všech správců front v rámci skupiny sdílení front.

Je-li přepínač zabezpečení zapnutý, provedou se kontroly zabezpečení přidružené k přepínači. Když je přepínač zabezpečení vypnutý, kontroly zabezpečení přidružené k přepínači jsou vynechány. Výchozí nastavení je, že jsou nastaveny všechny přepínače zabezpečení.

z/OS *Přepínače a třídy*

Když spustíte správce front nebo aktualizujete zabezpečení, produkt IBM MQ nastaví přepínače podle stavu různých tříd RACF .

Když je spuštěn správce front (nebo když je třída MQADMIN nebo MXADMIN aktualizována příkazem IBM MQ REFRESH SECURITY), produkt IBM MQ nejprve zkontroluje stav RACF a odpovídající třídu:

- Třída MQADMIN, pokud používáte profily psané velkými písmeny
- Třída MXADMIN, pokud používáte profil smíšených případů.

Nastaví vypnutí zabezpečení subsystému, pokud je některá z těchto podmínek pravdivá:

- Produkt RACF je neaktivní nebo není nainstalován.
- Třída MQADMIN nebo MXADMIN není definována (tyto třídy jsou vždy definovány pro RACF , protože jsou zahrnuty v tabulce deskriptoru tříd (CDT)).
- Třída MQADMIN nebo MXADMIN nebyla aktivována.

Pokud jsou aktivní jak třída RACF , tak třída MQADMIN nebo MXADMIN, produkt IBM MQ zkontroluje třídu MQADMIN nebo MXADMIN, aby zjistil, zda byl definován některý z profilů přepínače. Nejprve zkontroluje profily popsané v části “Profily pro řízení zabezpečení subsystému” na stránce 190. Pokud není vyžadováno zabezpečení subsystému, produkt IBM MQ nastaví vypnutí vnitřního zabezpečení subsystému a neprovede žádné další kontroly.

Profily určují, zda je odpovídající přepínač IBM MQ zapnutý nebo vypnutý.

- Je-li přepínač vypnutý, je tento typ zabezpečení deaktivován.
- Je-li nějaký přepínač IBM MQ zapnutý, IBM MQ zkontroluje stav třídy RACF přidružené k typu zabezpečení odpovídajícímu přepínači IBM MQ . Není-li třída nainstalována nebo není-li aktivní, je přepínač IBM MQ nastaven na hodnotu off (vypnuto). Kontroly zabezpečení procesu se například

neprovádějí, pokud nebyla aktivována třída MQPROC nebo MXPROC. Třída, která není aktivní, je ekvivalentní definování hodnoty NO.PROCESS.CHECKS pro každého správce front a skupinu sdílení front, která používá tuto databázi RACF .

z/OS *Jak přepínače fungují*

Chcete-li vypnout přepínač zabezpečení, definujte NO.* profil přepínače pro něj. Můžete přepsat NO.* profil nastavený na úrovni skupiny sdílení front definováním hodnoty YES.* profil pro správce front.

Chcete-li vypnout přepínač zabezpečení, musíte definovat hodnotu NO.* profil přepínače pro něj. Existence NO.* profil znamená, že pro daný typ prostředku **nejsou** prováděny kontroly zabezpečení, pokud se nerozhodnete přepsat nastavení úrovně skupiny sdílení front v konkrétním správci front. To je popsáno v tématu "Potlačení nastavení úrovně skupiny sdílení front" na stránce 190.

Pokud váš správce front není členem skupiny sdílení front, není nutné definovat žádné profily na úrovni skupiny sdílení front ani žádné profily potlačení. Tyto profily je však třeba definovat v případě, že se správce front později připojí ke skupině sdílení front.

Každé NO.* Profil přepínače, který produkt IBM MQ zjistí, vypne kontrolu pro tento typ prostředku. Profily přepínače jsou aktivovány během spouštění správce front. Změníte-li profily přepínače v době, kdy jsou spuštěni ovlivnění správci front, můžete produkt IBM MQ rozpoznat změny zadáním příkazu IBM MQ REFRESH SECURITY.

Profily přepínače musí být vždy definovány ve třídě MQADMIN nebo MXADMIN. Nedefinujte je ve třídě GMQADMIN nebo GMXADMIN. Tabulky Přepnout profily pro zabezpečení na úrovni subsystému a Přepnout profily pro kontrolu prostředků zobrazují platné profily přepínače a typ zabezpečení, které řídí.

Potlačení nastavení úrovně skupiny sdílení front

Můžete přepsat nastavení zabezpečení na úrovni skupiny sdílení front pro konkrétního správce front, který je členem této skupiny. Chcete-li provádět kontroly jednotlivých správců front, které nejsou prováděny na jiných správcích front ve skupině, použijte volbu (qmgr-name.YES. *) profily přepínače.

Naopak, pokud nechcete provést určitou kontrolu jednoho konkrétního správce front v rámci skupiny sdílení front, definujte (qmgr-name.NO. *) profil pro konkrétní typ prostředku ve správci front a nedefinuje profil pro skupinu sdílení front. (Produkt IBM MQ kontroluje pouze profil na úrovni skupiny sdílení front, pokud nenajde profil na úrovni správce front.)

z/OS *Profily pro řízení zabezpečení subsystému*

Produkt IBM MQ kontroluje, zda jsou vyžadovány kontroly zabezpečení subsystému pro subsystém, správce front a skupinu sdílení front.

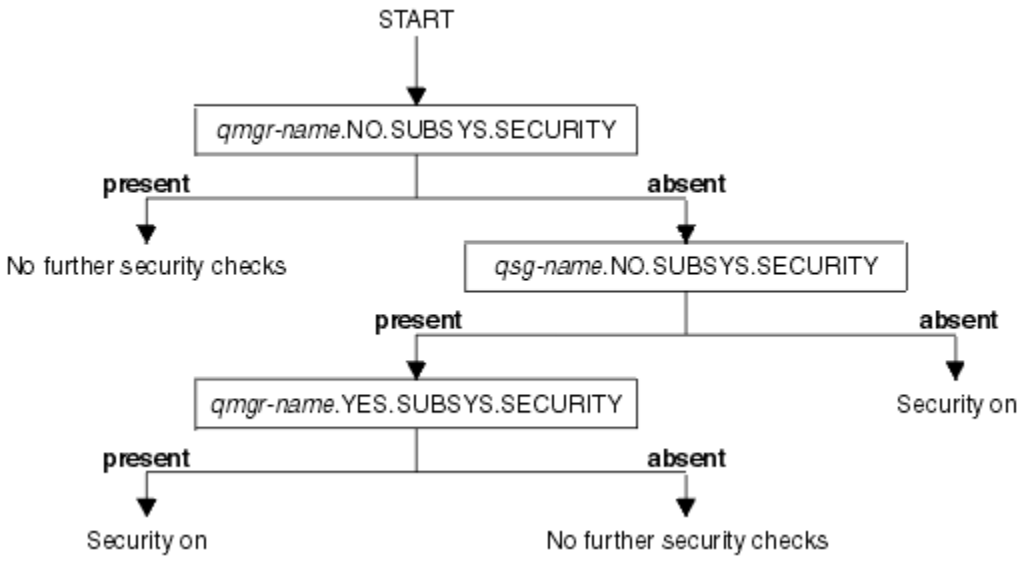
První kontrola zabezpečení prováděná produktem IBM MQ se používá k určení, zda jsou vyžadovány kontroly zabezpečení pro celý subsystém IBM MQ . Pokud určíte, že nechcete zabezpečení subsystému, nebudou provedeny žádné další kontroly.

Následující profily přepínače se kontrolují, aby se zjistilo, zda je vyžadováno zabezpečení subsystému. Obrázek 14 na stránce 191 zobrazuje pořadí, ve kterém jsou zaškrtnuty.

Tabulka 24. Profily přepínače pro zabezpečení na úrovni subsystému

Název profilu přepínače	**Typ prostředku nebo kontrolovaná kontrola**
qmgr-name.NO.SUBSYS.SECURITY	Zabezpečení subsystému pro tohoto správce front
qsg-name.NO.SUBSYS.SECURITY	Zabezpečení subsystému pro tuto skupinu sdílení front
qmgr-name.YES.SUBSYS.SECURITY	Potlačení zabezpečení subsystému pro tohoto správce front

Pokud váš správce front není členem skupiny sdílení front, produkt IBM MQ zkontroluje pouze profil přepínače qmgr-name.NO.SUBSYS.SECURITY .



Obrázek 14. Kontrola zabezpečení subsystému

z/OS *Profily pro řízení skupiny sdílení front nebo zabezpečení na úrovni správce front*

Je-li vyžadována kontrola zabezpečení subsystému, produkt IBM MQ zkontroluje, zda je vyžadována kontrola zabezpečení na úrovni skupiny sdílení front nebo správce front.

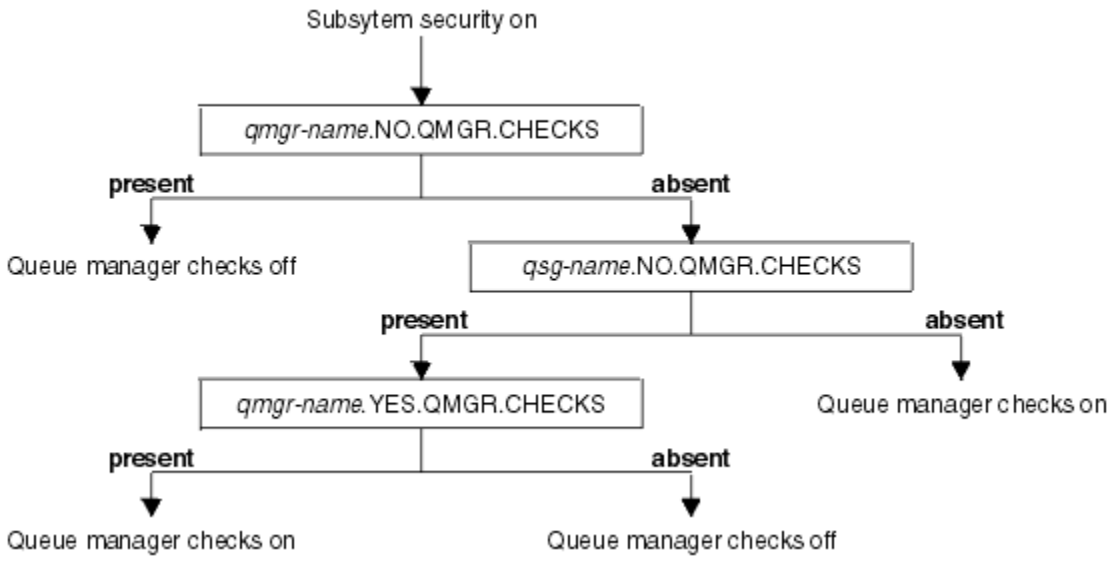
Pokud produkt IBM MQ zjistí, že je vyžadována kontrola zabezpečení, určí, zda je vyžadována kontrola na úrovni skupiny sdílení front nebo správce front, nebo na obou úrovních. Tyto kontroly se neprovádějí, pokud váš správce front není členem skupiny sdílení front.

Následující profily přepínače se kontrolují, aby se určila požadovaná úroveň. Obrázek 15 na stránce 192 a Obrázek 16 na stránce 192 zobrazují pořadí, ve kterém jsou zaškrtnuty.

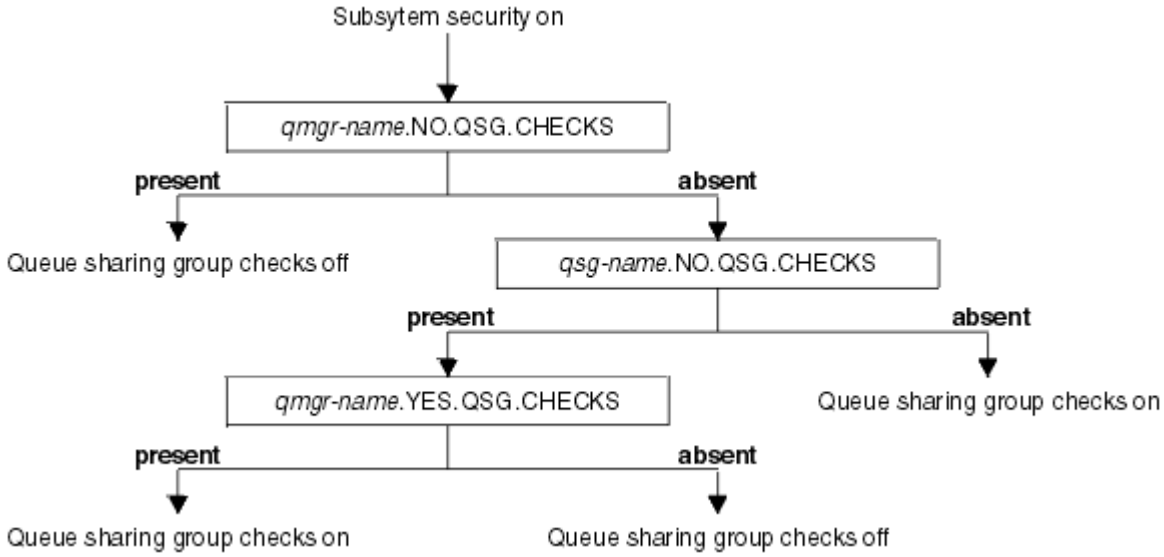
Tabulka 25. Profily přepínače pro skupinu sdílení front nebo zabezpečení na úrovni správce front

Název profilu přepínače	**Typ prostředku nebo kontrolovaná kontrola**
qmgr-name.NO.QMGR.CHECKS	Pro tohoto správce front nejsou k dispozici žádné kontroly na úrovni správce front.
qsg-name.NO.QMGR.CHECKS	Pro tuto skupinu sdílení front nejsou k dispozici žádné kontroly na úrovni správce front.
qmgr-name.YES.QMGR.CHECKS	Potlačení kontrol na úrovni správce front pro tohoto správce front
qmgr-name.NO.QSG.CHECKS	Pro tohoto správce front nejsou k dispozici žádné kontroly na úrovni skupiny sdílení front.
qsg-name.NO.QSG.CHECKS	Pro tuto skupinu sdílení front nejsou k dispozici žádné kontroly na úrovni skupiny sdílení front.
qmgr-name.YES.QSG.CHECKS	Potlačení kontrol na úrovni skupiny sdílení front pro tohoto správce front

Je-li zabezpečení subsystému aktivní, nelze vypnout zabezpečení na úrovni skupiny sdílení front ani zabezpečení na úrovni správce front. Pokusíte-li se tak učinit, produkt IBM MQ nastaví kontrolu zabezpečení na obou úrovních.



Obrázek 15. Kontrola zabezpečení na úrovni správce front



Obrázek 16. Kontrola zabezpečení na úrovni skupiny sdílení front

z/OS *Platné kombinace bezpečnostních přepínačů*

Platné jsou pouze určité kombinace přepínačů. Pokud použijete neplatnou kombinaci nastavení přepínače, bude vydána zpráva CSQH026I a kontrola zabezpečení bude nastavena na úrovni skupiny sdílení front i správce front.

Tabulka 26 na stránce 192, Tabulka 27 na stránce 193, Tabulka 28 na stránce 193a Tabulka 29 na stránce 194 zobrazují sady kombinací nastavení přepínače, které jsou platné pro každý typ úrovně zabezpečení.

Tabulka 26. Platné kombinace přepínačů zabezpečení pro zabezpečení na úrovni správce front
Kombinace
qmgr-name.NO.QSG.CHECKS
qsg-name.NO.QSG.CHECKS

Tabulka 26. Platné kombinace přepínačů zabezpečení pro zabezpečení na úrovni správce front (pokračování)

Kombinace
qmgr-name.NO.QSG.CHECKS qsg-name.NO.QMGR.CHECKS qmgr-name.YES.QMGR.CHECKS
qsg-name.NO.QSG.CHECKS qsg-name.NO.QMGR.CHECKS qmgr-name.YES.QMGR.CHECKS

Tabulka 27. Platné kombinace přepínačů zabezpečení pro zabezpečení na úrovni skupiny sdílení front

Kombinace
qmgr-name.NO.QMGR.CHECKS
qsg-name.NO.QMGR.CHECKS
qmgr-name.NO.QMGR.CHECKS qsg-name.NO.QSG.CHECKS qmgr-name.YES.QSG.CHECKS
qsg-name.NO.QMGR.CHECKS qsg-name.NO.QSG.CHECKS qmgr-name.YES.QSG.CHECKS

Tabulka 28. Platné kombinace přepínačů zabezpečení pro zabezpečení na úrovni správce front a skupiny sdílení front

Kombinace
qsg-name.NO.QMGR.CHECKS qmgr-name.YES.QMGR.CHECKS Žádné QSG.* definované profily
Žádné QMGR.* definované profily qsg-name.NO.QSG.CHECKS qmgr-name.YES.QSG.CHECKS
qsg-name.NO.QMGR.CHECKS qmgr-name.YES.QMGR.CHECKS qsg-name.NO.QSG.CHECKS qmgr-name.YES.QSG.CHECKS
Nejsou definovány žádné profily pro žádný přepínač

*Tabulka 29. Další platné kombinace přepínačů zabezpečení, které přepínají obě úrovně kontroly **na systému**.*
Kombinace
qmgr-name.NO.QMGR.CHECKS qmgr-name.NO.QSG.CHECKS
qsg-name.NO.QMGR.CHECKS qsg-name.NO.QSG.CHECKS
qmgr-name.NO.QMGR.CHECKS qsg-name.NO.QSG.CHECKS
qsg-name.NO.QMGR.CHECKS qmgr-name.NO.QSG.CHECKS

z/OS *Kontroly úrovně prostředků*

K řízení přístupu k prostředkům se používá řada profilů přepínačů. Některá zastavení kontroly prováděná ve správci front nebo ve skupině sdílení front. Ty lze přepsat profily, které umožňují kontrolu specifických správců front.

Tabulka 30 na stránce 194 zobrazuje profily přepínače použité k řízení přístupu k prostředkům IBM MQ .

Pokud je váš správce front součástí skupiny sdílení front a máte aktivní zabezpečení správce front i skupiny sdílení front, můžete použít YES.* Přepněte profil tak, aby potlačil profily na úrovni skupiny sdílení front, a specificky zapněte zabezpečení pro konkrétního správce front.

Některé profily se vztahují jak na správce front, tak na skupiny sdílení front. Tyto předpony jsou uvedeny řetězcem *hlq* a měli byste případně nahradit název skupiny sdílení front nebo správce front. Názvy profilů zobrazené s předponou *qmgr-name* jsou profily potlačení správce front; měli byste nahradit název svého správce front.

Tabulka 30. Přepnout profily pro kontrolu prostředků

Typ řízené kontroly prostředků	**Název profilu přepínače**	**Přepsat profil pro konkrétního správce front**
Zabezpečení připojení	hlq.NO.CONNECT.CHECKS	qmgr-name.YES.CONNECT.CHECKS
Zabezpečení fronty	hlq.NO.QUEUE.CHECKS	qmgr-name.YES.QUEUE.CHECKS
Zabezpečení procesů	hlq.NO.PROCESS.CHECKS	qmgr-name.YES.PROCESS.CHECKS
Zabezpečení seznamu názvů	hlq.NO.NLIST.CHECKS	qmgr-name.YES.NLIST.CHECKS
zabezpečení kontextu	hlq.NO.CONTEXT.CHECKS	qmgr-name.YES.CONTEXT.CHECKS
alternativní zabezpečení uživatele	hlq.NO.ALTERNATE.USER.CHECKS	qmgr-name.YES.ALTERNATE.USER.CHECKS
Zabezpečení příkazů	hlq.NO.CMD.CHECKS	qmgr-name.YES.CMD.CHECKS
Zabezpečení prostředků příkazu	hlq.NO.CMD.RESC.CHECKS	qmgr-name.YES.CMD.RESC.CHECKS

Tabulka 30. Přepnout profily pro kontrolu prostředků (pokračování)		
Typ řízené kontroly prostředků	**Název profilu přepínače**	**Přepsat profil pro konkrétního správce front**
Zabezpečení tématu	hlq.NO.TOPIC.CHECKS	qmgr-name.YES.TOPIC.CHECKS
Poznámka: Generické profily přepínače, jako např. hlq.NO. * * jsou ignorovány pomocí IBM MQ		

Chcete-li například provádět kontroly zabezpečení procesů pro správce front QM01, který je členem skupiny sdílení front QSG3 , ale nechcete provádět kontroly zabezpečení procesů pro žádného z ostatních správců front ve skupině, definujte následující profily přepínače:

```
QSG3.NO.PROCESS.CHECKS
QM01.YES.PROCESS.CHECKS
```

Chcete-li provádět kontroly zabezpečení fronty pro všechny správce front ve skupině sdílení front s výjimkou QM02, definujte následující profil přepínače:

```
QM02.NO.QUEUE.CHECKS
```

(Není třeba definovat profil pro skupinu sdílení front, protože kontroly jsou automaticky povoleny, pokud není definován žádný profil.)

z/OS *Příklad definování přepínačů*

Různé subsystémy IBM MQ mají různé požadavky na zabezpečení, které lze implementovat pomocí různých profilů přepínače.

Byly definovány čtyři subsystémy IBM MQ :

- MQP1 (produkční systém)
- MQP2 (produkční systém)
- MQD1 (vývojový systém)
- MQT1 (testovací systém)

Všichni čtyři správci front jsou členy skupiny sdílení front QS01. Všechny třídy produktu IBM MQ RACF byly definovány a aktivovány.

Tyto subsystémy mají různé požadavky na zabezpečení:

- Produkční systémy vyžadují úplnou kontrolu zabezpečení IBM MQ , aby byly aktivní na úrovni skupiny sdílení front na obou systémech.

  To se provádí zadáním následujícího profilu:

  ```
  RDEFINE MQADMIN QS01.NO.QMGR.CHECKS
  ```

  Tato volba nastaví kontrolu úrovně skupiny sdílení front pro všechny správce front ve skupině sdílení front. Nemusíte definovat žádné jiné profily přepínače pro produkční správce front, protože chcete zkontrolovat vše pro tyto systémy.
- Správce front testu MQT1 také vyžaduje úplnou kontrolu zabezpečení. Protože však může být vhodné toto změnit později, lze zabezpečení definovat na úrovni správce front tak, aby bylo možné změnit nastavení zabezpečení pro tohoto správce front bez ovlivnění ostatních členů skupiny sdílení front.

  To se provádí definováním hodnoty NO.QSG.CHECKS pro MQT1 :

  ```
  RDEFINE MQADMIN MQT1.NO.QSG.CHECKS
  ```

- Správce front vývoje MQD1 má jiné požadavky na zabezpečení než zbytek skupiny sdílení front. Vyžaduje pouze připojení a zabezpečení fronty, aby bylo aktivní.

  To se provádí definováním profilu `MQD1.YES.QMGR.CHECKS` pro tohoto správce front a následným definováním následujících profilů pro vypnutí kontroly zabezpečení pro prostředky, které není třeba kontrolovat:

```
RDEFINE MQADMIN MQD1.NO.CMD.CHECKS
RDEFINE MQADMIN MQD1.NO.CMD.RESC.CHECKS
RDEFINE MQADMIN MQD1.NO.PROCESS.CHECKS
RDEFINE MQADMIN MQD1.NO.NLIST.CHECKS
RDEFINE MQADMIN MQD1.NO.CONTEXT.CHECKS
RDEFINE MQADMIN MQD1.NO.ALTERNATE.USER.CHECKS
```

Je-li správce front aktivní, můžete zobrazit aktuální nastavení zabezpečení zadáním příkazu DISPLAY SECURITY MQSC.

Můžete také změnit nastavení přepínače, když je správce front spuštěn, definováním nebo odstraněním příslušného profilu přepínače ve třídě MQADMIN. Chcete-li provést změny nastavení přepínače aktivní, musíte zadat příkaz REFRESH SECURITY pro třídu MQADMIN.

Další podrobnosti o použití příkazů DISPLAY SECURITY a REFRESH SECURITY naleznete v části “Aktualizace zabezpečení správce front v systému z/OS” na stránce 250 .

z/OS Profily používané k řízení přístupu k prostředkům IBM MQ

Kromě profilů přepínače, které mohly být definovány, musíte definovat profily RACF pro řízení přístupu k prostředkům IBM MQ . Tato kolekce témat obsahuje informace o profilech RACF pro různé typy prostředků IBM MQ .

Pokud nemáte definován profil prostředku pro konkrétní kontrolu zabezpečení a uživatel vydá požadavek, který by zahrnoval provedení této kontroly, produkt IBM MQ odepře přístup. Nemusíte definovat profily pro typy zabezpečení související s jakýmikoli přepínači zabezpečení, které jste deaktivovali.

z/OS *Profily pro zabezpečení připojení*

Je-li zabezpečení připojení aktivní, musíte definovat profily ve třídě MQCONN a povolit potřebným skupinám nebo ID uživatelů přístup k těmto profilům, aby se mohli připojit k produktu IBM MQ.

Chcete-li povolit vytvoření připojení, musíte udělit uživatelům RACF přístup pro čtení k příslušnému profilu. (Pokud neexistuje žádný profil na úrovni správce front a váš správce front je členem skupiny sdílení front, může být provedena kontrola profilů na úrovni skupiny sdílení front, pokud je nastaveno zabezpečení.)

Profil připojení kvalifikovaný názvem správce front řídí přístup ke specifickému správci front a uživatelé, kterým byl udělen přístup k tomuto profilu, se k tomuto správci front mohou připojit. Profil připojení kvalifikovaný názvem skupiny sdílení front řídí přístup ke všem správcům front v rámci skupiny sdílení front pro daný typ připojení. Například uživatel s přístupem k produktu `QS01.BATCH` může použít dávkové připojení k libovolnému správci front ve skupině sdílení front QS01 , který nemá definovaný profil úrovně správce front.

Poznámka:

1. Informace o ID uživatelů, která jsou kontrolována pro různé požadavky na zabezpečení, viz “ID uživatelů pro kontrolu zabezpečení na systému z/OS” na stránce 239.
2. Kontroly zabezpečení na úrovni prostředku (RESLEVEL) se provádějí také v době připojení. Podrobné informace naleznete v tématu “Profil zabezpečení RESLEVEL” na stránce 233.

Zabezpečení produktu IBM MQ rozpoznává následující různé typy připojení:

- Dávková (a dávková) připojení zahrnují:
  - z/OS Dávkové úlohy
  - Aplikace TSO

  - z/OS UNIX System Services přihlášení
  - Db2Uložené procedury
- CICS připojení
- IMS připojení z oblastí řízení a zpracování aplikací
- Iniciátor kanálu IBM MQ

z/OS *Profily zabezpečení připojení pro dávková připojení*

Profily pro kontrolu připojení dávkového typu se skládají z názvu správce front nebo skupiny sdílení front následovaného slovem *BATCH*. Poskytněte ID uživatele přidruženému k připojovacímu adresnímu prostoru přístup READ k profilu připojení.

Profily pro kontrolu dávkových a dávkových připojení jsou ve tvaru:

```
hlq.BATCH
```

kde `hlq` může být buď `qmgr-name` (název správce front), nebo `qsg-name` (název skupiny sdílení front). Pokud používáte zabezpečení na úrovni správce front i skupiny sdílení front, produkt IBM MQ zkontroluje profil s předponou podle názvu správce front. Pokud jej nenajde, vyhledá profil s předponou názvu skupiny sdílení front. Pokud se mu nepodaří najít některý z profilů, požadavek na připojení se nezdaří.

Pro požadavky na připojení dávkového nebo dávkového typu musíte povolit ID uživatele přidružené k připojovacímu adresnímu prostoru pro přístup k profilu připojení. Například následující příkaz RACF umožňuje uživatelům ve skupině CONNTQM1 připojit se ke správci front TQM1; tato ID uživatelů budou mít povoleno používat jakékoli dávkové připojení nebo připojení dávkového typu.

```
RDEFINE MQCONN TQM1.BATCH UACC(NONE)
PERMIT TQM1.BATCH CLASS(MQCONN) ID(CONNTQM1) ACCESS(READ)
```

z/OS *Použití produktu **CHCKLOCL** v lokálně vázaných aplikacích*

CHCKLOCL platí pouze pro připojení, která jsou vytvořena prostřednictvím připojení BATCH a nevztahují se na připojení z produktu CICS nebo IMS. Připojení prostřednictvím inicializátoru kanálu jsou řízena produktem **CHCKCLNT**.

Přehled

Chcete-li nakonfigurovat správce front produktu z/OS tak, aby pro některé, ale ne pro všechny lokálně vázané aplikace vyžadoval kontrolu ID uživatele a hesla, je třeba provést další konfiguraci.

Důvodem je skutečnost, že po konfiguraci produktu **CHCKLOCL** (*REQUIRED*) se starší dávkové aplikace, které používají volání rozhraní API MQCONN, již nemohou připojit ke správci front.

Pouze pro systém z/OS lze použít podrobnější mechanizmus založený na zabezpečení připojení adresního prostoru ke snížení úrovně globální konfigurace CHCKLOCL (REQUIRED) na CHCKLOCL (OPTIONAL) pro specificky definovaná ID uživatelů. Použitý mechanismus je popsán v následujícím textu spolu s příkladem.

Chcete-li povolit větší granularitu v systému **CHCKLOCL** (*REQUIRED*) než jen pro EVERYONE, upravíte soubor **CHCKLOCL** stejným způsobem, jako upravíte úroveň přístupu ID uživatele přidruženého k připojovacímu adresnímu prostoru k profilům připojení `hlq.batch` ve třídě MQCONN.

Pokud má ID uživatele adresního prostoru pouze přístup READ, což je minimum, které potřebujete k tomu, abyste se mohli vůbec připojit, použije se konfigurace **CHCKLOCL** tak, jak byla napsána.

Pokud má ID uživatele adresního prostoru přístup UPDATE (nebo vyšší), pak konfigurace **CHCKLOCL** pracuje v režimu *OPTIONAL* . To znamená, že nemusíte zadávat ID uživatele a heslo, ale pokud tak učiníte, ID uživatele a heslo musí být platná dvojice.

Zabezpečení připojení je již konfigurováno pro vašeho správce front z/OS .

Máte-li nakonfigurováno zabezpečení připojení pro svého správce front z/OS a chcete, aby produkt **CHCKLOCL** (*REQUIRED*) platil pro lokálně vázané aplikace WAS a žádné další, postupujte takto:

1. Jako konfiguraci začněte s volbou **CHCKLOCL** (*VOLITELNĚ*). To znamená, že jakékoli ID uživatele a hesla, která jsou dodána, jsou ověřena na platnost, ale nejsou nařízena.
2. Zadáním příkazu vypište všechny uživatele, kteří mají přístup k profilům zabezpečení připojení:

   ```
   RLIST MQCONN MQ23.BATCH AUTHUSER
   ```

   Tento příkaz zobrazí například:

   ```
   CLASS    NAME
   -----    ----
   MQCONN   MQ23.BATCH

   USER     ACCESS  ACCESS COUNT
   ----     ------  ------ -----
   JOHNDOE  READ    000009
   JDOE1    READ    000003
   WASUSER  READ    000000
   ```

3. Pro každé ID uživatele uvedené jako ID, které má přístup pro čtení, změňte přístup na

   ```
   UPDATE:- PERMIT MQ23.BATCH CLASS(MQCONN) ID(JOHNDOE) ACCESS(UPDATE)
   ```

4. Aktualizujte konfiguraci IBM MQ na **CHCKLOCL** (*REQUIRED*).

   Kombinace přístupu UPDATE k souboru `MQ23.BATCH` a aktuálního nastavení znamená, že používáte zařízení **CHCKLOCL** (*OPTIONAL*).
5. Nyní použijte chování **CHCKLOCL** (*REQUIRED*) na jedno specifické ID uživatele, například `WASUSER`, aby všechna připojení přicházející z této oblasti musela poskytnout ID uživatele a heslo.

   Proveďte to tak, že obrátíte změnu, kterou jste provedli dříve, zadáním příkazu:

   ```
   PERMIT MQ23.BATCH CLASS(MQCONN) ID(WASUSER) ACCESS(READ)
   ```

Pro vašeho správce front z/OS není konfigurováno zabezpečení připojení.

V této situaci musíte:

1. Vytvořte profily připojení pro produkt `hlq.BATCH` ve třídě MQCONN zadáním příkazu:

   ```
   RDEFINE MQCONN MQ23.BATCH UACC(NONE)
   ```

2. Autorizujte všechna ID uživatelů, kteří vytvářejí dávková připojení ke správci front, aby měli k tomuto profilu přístup UPDATE. Tímto se vynechá požadavek **CHCKLOCL** (*REQUIRED*) pro ID uživatele a heslo v době připojení.

   Proveďte to zadáním příkazu:

   ```
   PERMIT MQ23.BATCH CLASS(MQCONN)ID(JOHNDOE) ACCESS(UPDATE)
   ```

   Mezi ně patří ID uživatelů:

   a. Používá se pro panely CSQUTIL, ISPF a další lokálně vázané nástroje.

   b. Přidruženo k dávkovým připojením typu like ke správci front. Zvažte například Advanced Message Security, IBM Integration Bus, Db2 uložené procedury, z/OS UNIX System Services a uživatele TSO a aplikace Java .

3. Odstraňte profil přepínače pro správce front zadáním příkazu:

```
hlq.NO.CONNECT.CHECKS
```

4. Nyní použijte chování **CHCKLOCL** (*REQUIRED*) na jedno specifické ID uživatele, například WASUSER, aby všechna připojení přicházející z této oblasti musela poskytnout ID uživatele a heslo.

   Proveďte to tak, že obrátíte změnu, kterou jste provedli dříve, zadáním příkazu:

```
PERMIT MQ23.BATCH CLASS(MQCONN) ID(WASUSER) ACCESS(READ)
```

z/OS *Profily zabezpečení připojení pro připojení CICS*

Profily pro kontrolu připojení produktu CICS se skládají z názvu správce front nebo skupiny sdílení front následovaného slovem *CICS* . Přidělte ID uživatele přidružené k adresnímu prostoru CICS přístup READ k profilu připojení.

Profily pro kontrolu připojení z produktu CICS jsou ve formátu:

```
hlq.CICS
```

kde `hlq` může být buď `qmgr-name` (název správce front), nebo `qsg-name` (název skupiny sdílení front). Pokud používáte zabezpečení na úrovni správce front i skupiny sdílení front, produkt IBM MQ zkontroluje profil s předponou podle názvu správce front. Pokud jej nenajde, vyhledá profil s předponou názvu skupiny sdílení front. Pokud nenajde některý z profilů, požadavek na připojení selže.

Pro požadavky na připojení od CICSmusíte povolit pouze přístup ID uživatele adresního prostoru CICS k profilu připojení.

Následující příkazy RACF například umožňují připojení ID uživatele adresního prostoru CICS KCBCICS ke správci front TQM1:

```
RDEFINE MQCONN TQM1.CICS UACC(NONE)
PERMIT TQM1.CICS CLASS(MQCONN) ID(KCBCICS) ACCESS(READ)
```

z/OS *Profily zabezpečení připojení pro připojení IMS*

Profily pro kontrolu připojení produktu IMS se skládají z názvu správce front nebo skupiny sdílení front následovaného slovem *IMS* . Udělte ID uživatele ovládacího prvku IMS a závislé oblasti přístup READ k profilu připojení.

Profily pro kontrolu připojení z produktu IMS jsou ve formátu:

```
hlq.IMS
```

kde `hlq` může být buď `qmgr-name` (název správce front), nebo `qsg-name` (název skupiny sdílení front). Pokud používáte zabezpečení na úrovni správce front i skupiny sdílení front, produkt IBM MQ zkontroluje profil s předponou podle názvu správce front. Pokud jej nenajde, vyhledá profil s předponou názvu skupiny sdílení front. Pokud nenajde některý z profilů, požadavek na připojení selže.

Pro požadavky na připojení od IMSpovolte přístup k profilu připojení pro ID uživatele ovládacího prvku IMS a závislé oblasti.

Následující příkazy RACF například umožňují:

- ID uživatele oblasti IMS IMSREG pro připojení ke správci front TQM1.

- Uživatelé ve skupině BMPGRP pro odeslání úloh BMP.

```
RDEFINE MQCONN TQM1.IMS UACC(NONE)
PERMIT TQM1.IMS CLASS(MQCONN) ID(IMSREG,BMPGRP) ACCESS(READ)
```

z/OS *Profily zabezpečení připojení pro inicializátor kanálu*

Profily pro kontrolu připojení z inicializátoru kanálu se skládají z názvu správce front nebo skupiny sdílení front následovaného slovem *CHIN*. Přidělte ID uživatele, které používá adresní prostor spuštěné úlohy inicializátoru kanálu, přístup READ k profilu připojení.

Profily pro kontrolu připojení z inicializátoru kanálu jsou ve tvaru:

```
hlq.CHIN
```

kde `hlq` může být buď `qmgr-name` (název správce front), nebo `qsg-name` (název skupiny sdílení front). Pokud používáte zabezpečení na úrovni správce front i skupiny sdílení front, produkt IBM MQ zkontroluje profil s předponou podle názvu správce front. Pokud jej nenajde, vyhledá profil s předponou názvu skupiny sdílení front. Pokud nenajde některý z profilů, požadavek na připojení selže.

Pro požadavky na připojení iniciátorem kanálu definujte přístup k profilu připojení pro ID uživatele použité adresním prostorem spuštěné úlohy inicializátoru kanálu.

Následující příkazy RACF například umožňují, aby se adresní prostor inicializátoru kanálu spuštěný s ID uživatele DQCTRL připojil ke správci front TQM1:

```
RDEFINE MQCONN TQM1.CHIN UACC(NONE)
PERMIT TQM1.CHIN CLASS(MQCONN) ID(DQCTRL) ACCESS(READ)
```

z/OS ***Profily pro zabezpečení fronty***

Je-li zabezpečení fronty aktivní, musíte definovat profily v odpovídajících třídách a povolit potřebným skupinám nebo ID uživatelů přístup k těmto profilům. Profily zabezpečení fronty jsou pojmenovány po správci front nebo skupině sdílení front a po frontě, která má být otevřena.

Je-li zabezpečení fronty aktivní, musíte:

- Definujte profily ve třídách **MQQUEUE** nebo **GMQQUEUE** , používáte-li profily s velkými písmeny.
- Definujte profily ve třídách **MXQUEUE** nebo **GMXQUEUE** , pokud používáte profily se smíšenými velkými a velkými písmeny.
- Povolte potřebné skupiny nebo ID uživatelů přístup k těmto profilům, aby mohli vydávat požadavky rozhraní IBM MQ API, které používají fronty.

Profily pro zabezpečení fronty jsou ve tvaru:

```
hlq.queuename
```

kde `hlq` může být buď `qmgr-name` (název správce front), nebo `qsg-name` (název skupiny sdílení front) a `queuename` je název fronty, která se otevírá, jak je uvedeno v deskriptoru objektu ve volání `MQOPEN` nebo `MQPUT1` .

Profil s předponou názvu správce front řídí přístup k jedné frontě v daném správci front. Profil s předponou názvu skupiny sdílení front řídí přístup k jedné nebo více frontám s tímto názvem ve všech správcích front v rámci skupiny sdílení front nebo přístup ke sdílené frontě libovolným správcem front v rámci skupiny.

Tento přístup lze přepsat v jednotlivém správci front definováním profilu úrovně správce front pro danou frontu v daném správci front.

Pokud je váš správce front členem skupiny sdílení front a používáte zabezpečení na úrovni správce front i skupiny sdílení front, produkt IBM MQ nejprve zkontroluje profil s předponou podle názvu správce front. Pokud jej nenajde, vyhledá profil s předponou názvu skupiny sdílení front.

Používáte-li sdílené fronty, doporučuje se používat zabezpečení na úrovni skupiny sdílení front.

Podrobnosti o tom, jak funguje zabezpečení fronty, když je název fronty alias nebo modelová fronta, viz “Aspekty pro fronty aliasů” na stránce 202 a “Aspekty pro modelové fronty” na stránce 203 .

Přístup RACF nezbytný k otevření fronty závisí na zadaných volbách MQOPEN nebo MQPUT1 . Pokud je kódována více než jedna z voleb MQOO_ * a MQPMO_ *, provede se kontrola zabezpečení fronty pro nejvyšší požadované oprávnění RACF .

Tabulka 31. Úrovně přístupu pro zabezpečení fronty pomocí volání MQOPEN nebo MQPUT1

Volba MQOPEN nebo MQPUT1	**RACF úroveň přístupu požadovaná pro hlq.queuename**
MQOO_BROWSE	READ (čtení)
MQOO_DOTAZOVAT	READ (čtení)
MQOO_BIND_ *	AKTUALIZOVAT
MQOO_INPUT_ *	AKTUALIZOVAT
MQOO_OUTPUT nebo MQPUT1	AKTUALIZOVAT
MQOO_PASS_ALL_CONTEXT MQPMO_PASS_ALL_CONTEXT	AKTUALIZOVAT
MQOO_PASS_IDENTITY_CONTEXT MQPMO_PASS_IDENTITY_CONTEXT	AKTUALIZOVAT
MQOO_SAVE_ALL_CONTEXT	AKTUALIZOVAT
MQOO_SET_IDENTITY_CONTEXT MQPMO_SET_IDENTITY_CONTEXT	AKTUALIZOVAT
MQOO_SET_ALL_CONTEXT MQPMO_SET_ALL_CONTEXT	AKTUALIZOVAT
MQOO_SET	ALTER

Například v IBM MQ správci front QM77mají být všem ID uživatelů ve skupině RACF PAYGRP udělen přístup pro získání zpráv ze všech front nebo pro vložení zpráv do všech front s názvy začínajícími na 'PAY.'. Můžete to provést pomocí těchto příkazů RACF :

```
RDEFINE MQQUEUE QM77.PAY.** UACC(NONE)
PERMIT QM77.PAY.** CLASS(MQQUEUE) ID(PAYGRP) ACCESS(UPDATE)
```

Také všechna ID uživatelů ve skupině PAYGRP musí mít přístup k vkládání zpráv do front, které nedodržují konvenci pojmenování PAY. Příklad:

```
REQUEST_QUEUE_FOR_PAYROLL
SALARY.INCREASE.SERVER
REPLIES.FROM.SALARY.MODEL
```

To lze provést definováním profilů pro tyto fronty ve třídě GMQQUEUE a poskytnutím přístupu k této třídě následujícím způsobem:

```
RDEFINE GMQQUEUE PAYROLL.EXTRAS UACC(NONE)
        ADDMEM(QM77.REQUEST_QUEUE_FOR_PAYROLL,
               QM77.SALARY.INCREASE.SERVER,
               QM77.REPLIES.FROM.SALARY.MODEL)
PERMIT PAYROLL.EXTRAS CLASS(GMQQUEUE) ID(PAYGRP) ACCESS(UPDATE)
```

Poznámka:

1. Dojde-li ke změně úrovně přístupu RACF , kterou má aplikace k profilu zabezpečení fronty, projeví se změny pouze pro všechny nově získané manipulátory objektů (tj. nové manipulátory MQOPEN) pro danou frontu. Tyto popisovače, které již existují v době změny, si zachovávají svůj stávající přístup k frontě. Pokud je aplikace povinna používat změněnou úroveň přístupu ke frontě, a nikoli existující úroveň přístupu, musí zavřít a znovu otevřít frontu pro každý popisovač objektu, který změnu vyžaduje.
2. V tomto příkladu může být název správce front QM77 také názvem skupiny sdílení front.

V době, kdy je fronta otevřena, se mohou vyskytnout i jiné typy kontrol zabezpečení, v závislosti na zadaných volbách otevření a na typech zabezpečení, které jsou aktivní. Viz také “Profily pro zabezpečení kontextu” na stránce 217 a “Profily pro alternativní zabezpečení uživatele” na stránce 216. Chcete-li zobrazit souhrnnou tabulku zobrazující volby otevření a autorizaci zabezpečení potřebnou pro aktivní zabezpečení fronty, kontextu a alternativního uživatele, prohlédněte si téma Tabulka 36 na stránce 208.

Pokud používáte publikování/odběr, musíte zvážit následující. Při zpracování požadavku MQSUB se provádí kontrola zabezpečení, aby se zajistilo, že ID uživatele, který zadal požadavek, má požadovaný přístup pro vložení zpráv do cílové fronty IBM MQ a také požadovaný přístup pro přihlášení k odběru tématu IBM MQ .

Tabulka 32. Úrovně přístupu pro zabezpečení fronty pomocí volání MQSUB

Volba MQSUB	**RACF úroveň přístupu požadovaná pro hlq.queuename**
MQSO_ALTER, MQSO_CREATE a MQSO_RESUME	AKTUALIZOVAT

Poznámka:

1. hlq.queuename je cílová fronta pro publikování. Jedná-li se o spravovanou frontu, potřebujete přístup k příslušné modelové frontě, která má být použita pro spravovanou frontu a vytvořenou dynamickou frontu.
2. Chcete-li rozlišovat mezi uživateli, kteří provádějí odběry, a uživateli, kteří načítají publikování z cílové fronty, můžete použít podobnou techniku pro cílovou frontu, kterou zadáte ve volání rozhraní API MQSUB.

z/OS *Aspekty pro fronty aliasů*

Když zadáte volání MQOPEN nebo MQPUT1 pro alias frontu, produkt IBM MQ provede kontrolu prostředků podle názvu fronty určeného ve volání deskriptoru objektu (MQOD). Nekontroluje, zda má uživatel povolen přístup k názvu cílové fronty.

Například alias fronty s názvem PAYROLL.REQUEST se interpretuje jako cílová fronta PAY.REQUEST. Je-li zabezpečení fronty aktivní, musíte mít oprávnění pouze pro přístup k frontě PAYROLL.REQUEST. Není provedena žádná kontrola, zda máte oprávnění pro přístup k frontě PAY.REQUEST.

z/OS *Použití front aliasů k rozlišení mezi požadavky MQGET a MQPUT*

Rozsah volání MQI dostupných na jedné úrovni přístupu může způsobit problém, pokud chcete omezit přístup k frontě tak, aby bylo povoleno pouze volání **MQPUT** nebo pouze volání **MQGET** . Frontu lze chránit definováním dvou aliasů, které se do této fronty interpretují: jednoho, který umožňuje aplikacím získávat zprávy z fronty, a druhého, který umožňuje aplikacím vkládat zprávy do fronty.

Následující text uvádí příklad, jak můžete definovat své fronty pro IBM MQ:

```
DEFINE QLOCAL(MUST_USE_ALIAS_TO_ACCESS) GET(ENABLED)
       PUT(ENABLED)

DEFINE QALIAS(USE_THIS_ONE_FOR_GETS) GET(ENABLED)
       PUT(DISABLED) TARGET(MUST_USE_ALIAS_TO_ACCESS)

DEFINE QALIAS(USE_THIS_ONE_FOR_PUTS) GET(DISABLED)
       PUT(ENABLED) TARGET(MUST_USE_ALIAS_TO_ACCESS)
```

Musíte také provést následující definice RACF :

```
RDEFINE MQQUEUE hlq.MUST_USE_ALIAS_TO_ACCESS UACC(NONE)
RDEFINE MQQUEUE hlq.USE_THIS_ONE_FOR_GETS UACC(NONE)
RDEFINE MQQUEUE hlq.USE_THIS_ONE_FOR_PUTS UACC(NONE)
```

Poté se ujistěte, že k frontě hlq.MUST_USE_ALIAS_TO_ACCESSnemají přístup žádní uživatelé a že k aliasu mají přístup odpovídající uživatelé nebo skupiny. To můžete provést pomocí následujících příkazů RACF :

```
PERMIT hlq.USE_THIS_ONE_FOR_GETS CLASS(MQQUEUE)
       ID(GETUSER,GETGRP) ACCESS(UPDATE)
PERMIT hlq.USE_THIS_ONE_FOR_PUTS CLASS(MQQUEUE)
       ID(PUTUSER,PUTGRP) ACCESS(UPDATE)
```

To znamená, že ID uživatele GETUSER a ID uživatele ve skupině GETGRP mohou získat zprávy pouze v MUST_USE_ALIAS_TO_ACCESS prostřednictvím alias fronty USE_THIS_ONE_FOR_GETS; a ID uživatele PUTUSER a ID uživatele ve skupině PUTGRP mají povoleno vkládat zprávy pouze prostřednictvím alias fronty USE_THIS_ONE_FOR_PUTS.

Poznámka:

1. Chcete-li použít techniku, jako je tato, musíte informovat vývojáře aplikací, aby mohli vhodně navrhnout své programy.
2. Chcete-li rozlišovat mezi uživateli, kteří provádějí odběry, a uživateli, kteří "získávají" publikování z cílové fronty, můžete použít techniku podobnou této pro cílovou frontu, kterou zadáte v požadavku rozhraní API MQSUB.

z/OS *Aspekty pro modelové fronty*

Chcete-li otevřít modelovou frontu, musíte být schopni otevřít samotnou modelovou frontu i dynamickou frontu, do které se tato fronta vyřeší. Definujte generické profily RACF pro dynamické fronty, včetně dynamických front používaných obslužnými programy IBM MQ .

Když otevřete modelovou frontu, zabezpečení produktu IBM MQ provede dvě kontroly zabezpečení fronty:

1. Máte oprávnění pro přístup k modelové frontě?
2. Jste autorizováni pro přístup k dynamické frontě, na kterou se modelová fronta interpretuje?

Pokud název dynamické fronty obsahuje koncový znak hvězdičky (*), je tento znak * nahrazen znakovým řetězcem generovaným produktem IBM MQ, aby se vytvořila dynamická fronta s jedinečným názvem. Protože se však pro kontrolu oprávnění používá celý název včetně tohoto generovaného řetězce, měli byste pro tyto fronty definovat generické profily.

Například volání MQOPEN používá název modelové fronty CREDIT.CHECK.REPLY.MODEL a název dynamické fronty CREDIT.REPLY.* ve správci front (nebo skupině sdílení front) MQSP.

Chcete-li to provést, musíte zadat následující příkazy RACF , abyste definovali nezbytné profily front:

```
RDEFINE MQQUEUE MQSP.CREDIT.CHECK.REPLY.MODEL
RDEFINE MQQUEUE MQSP.CREDIT.REPLY.**
```

Musíte také zadat odpovídající příkazy RACF PERMIT, abyste uživateli povolili přístup k těmto profilům.

Typický název dynamické fronty vytvořený pomocí MQOPEN je podobný názvu CREDIT.REPLY.A346EF00367849A0. Přesná hodnota posledního kvalifikátoru je nepředvídatelná; proto byste měli pro tyto názvy front používat generické profily.

Počet obslužných programů systému IBM MQ vkládal zprávy do dynamických front. Měli byste definovat profily pro následující názvy dynamických front a poskytnout přístup RACF UPDATE k příslušným ID uživatelů (správná ID uživatelů viz "ID uživatelů pro kontrolu zabezpečení na systému z/OS" na stránce 239):

```
SYSTEM.CSQUTIL.*  (used by CSQUTIL)
SYSTEM.CSQOREXX.* (used by the operations and control panels)
SYSTEM.CSQXCMD.*  (used by the channel initiator when processing CSQINPX)
CSQ4SAMP.*        (used by the IBM MQ supplied samples)
```

Můžete také zvážit definování profilu pro řízení použití názvu dynamické fronty, který se standardně používá ve členech kopie programování aplikací. IBM MQ-dodané zakladače obsahují výchozí *DynamicQName*, což je CSQ. *. To umožňuje vytvoření příslušného profilu RACF .

Poznámka: Nepovolit aplikačním programátorům zadat pro název dynamické fronty jeden znak *. Pokud tak učiníte, musíte definovat hlq. * * profil ve třídě MQQUEUE a měli byste mu poskytnout široký přístup. To znamená, že tento profil lze použít i pro jiné nedynamické fronty, které nemají specifičtější profil RACF . Uživatelé tak mohou získat přístup k frontám, ke kterým nemají přístup.

z/OS *Zavřít volby v trvalých dynamických frontách*

Pokud aplikace otevře trvalou dynamickou frontu, která byla vytvořena jinou aplikací, a poté se pokusí odstranit tuto frontu pomocí volby MQCLOSE , budou při pokusu provedeny některé další kontroly zabezpečení.

Tabulka 33. Úrovně přístupu pro volby zavření v trvalých dynamických frontách

Volba MQCLOSE	**RACF úroveň přístupu požadovaná pro hlq.queuename**
MQCO_DELETE	ALTER
MQCO_DELETE_PURGE	ALTER

z/OS *Zabezpečení a vzdálené fronty*

Při vložení zprávy do vzdálené fronty závisí zabezpečení fronty implementované lokálním správcem front na způsobu zadání vzdálené fronty při jejím otevření.

Použijí se následující pravidla:

1. Pokud byla vzdálená fronta definována v lokálním správci front pomocí příkazu IBM MQ DEFINE QREMOTE, je kontrolovaná fronta názvem vzdálené fronty. Pokud je například ve správci front MQS1 definována vzdálená fronta, postupujte takto:

   ```
   DEFINE QREMOTE(BANK7.CREDIT.REFERENCE)
          RNAME(CREDIT.SCORING.REQUEST)
          RQMNAME(BNK7)
          XMITQ(BANK1.TO.BANK7)
   ```

   V tomto případě profil pro BANK7.CREDIT.REFERENCE musí být definována ve třídě MQQUEUE.
2. Pokud se název *ObjectQMgr* pro požadavek nevyřeší na lokálního správce front, provede se kontrola zabezpečení pro vyřešený (vzdálený) název správce front s výjimkou případu, kdy je provedena kontrola pro název fronty klastru.

   Například přenosová fronta BANK1.TO.BANK7 je definován ve správci front MQS1. Požadavek MQPUT1 je poté vydán na MQS1 s uvedením *ObjectName* jako BANK1.INTERBANK.TRANSFERS

a *ObjectQMgrNázev* BANK1.TO.BANK7. V tomto případě musí mít uživatel provádějící požadavek přístup k BANK1.TO.BANK7.

3. Pokud provedete požadavek MQPUT do fronty a zadáte *ObjectQMgrName* jako název aliasu lokálního správce front, bude kontrolováno pouze zabezpečení názvu fronty, nikoli zabezpečení správce front.

Když se zpráva dostane do vzdáleného správce front, může být předmětem dalšího zpracování zabezpečení. Další informace viz téma “Zabezpečení pro vzdálený systém zpráv” na stránce 100.

z/OS *Zabezpečení fronty nedoručených zpráv*

Pro frontu nedoručených zpráv platí zvláštní pokyny, protože mnoho uživatelů musí být schopno do ní vkládat zprávy, ale přístup k načítacím zprávám musí být přísně omezen. Toho lze dosáhnout použitím různých oprávnění RACF pro frontu nedoručených zpráv a alias fronty.

Nedoručené zprávy lze vložit do speciální fronty nazvané fronta nedoručených zpráv. Pokud máte citlivá data, která by mohla skončit v této frontě, musíte zvážit důsledky pro zabezpečení, protože nechcete, aby tato data načítali neautorizovaní uživatelé.

Pro vložení zpráv do fronty nedoručených zpráv musí být povolena každá z následujících možností:

- Aplikační programy.
- Adresní prostor inicializátoru kanálu a všechna ID uživatelů MCA. (Pokud profil RESLEVEL není přítomen nebo je definován tak, aby byla kontrolována ID uživatele kanálu, potřebuje ID uživatele kanálu také oprávnění pro vložení zpráv do fronty nedoručených zpráv.)
- CKTI, iniciátor úlohy CICS-dodaný CICS .
- CSQQTRMN, monitor spouštěčů IBM MQ-dodaný IMS .

Jedinou aplikací, která může načíst zprávy z fronty nedoručených zpráv, by měla být 'speciální' aplikace, která tyto zprávy zpracovává. Problém však nastává, pokud dáte aplikacím oprávnění RACF UPDATE k frontě nedoručených zpráv pro MQPUT , protože pak mohou automaticky načítat zprávy z fronty pomocí volání MQGET . Nemůžete zakázat frontu nedoručených zpráv pro operace get, protože pokud tak učiníte, ani 'speciální' aplikace nemohou načíst zprávy.

Jedním z řešení tohoto problému je nastavení dvouúrovňového přístupu k frontě nedoručených zpráv. CKTI, transakce agenta kanálu zpráv nebo adresní prostor inicializátoru kanálu a 'speciální' aplikace mají přímý přístup; ostatní aplikace mohou přistupovat k frontě nedoručených zpráv pouze prostřednictvím alias fronty. Tento alias je definován tak, aby umožňoval aplikacím vkládat zprávy do fronty nedoručených zpráv, ale nikoli z ní získávat zprávy.

Takto by to mohlo fungovat:

1. Definujte skutečnou frontu nedoručených zpráv s atributy PUT (ENABLED) a GET (ENABLED), jak je zobrazeno v ukázce thlqual.SCSQPROC(CSQ4INYG).
2. Poskytněte oprávnění RACF UPDATE pro frontu nedoručených zpráv následujícím ID uživatelů:
   - ID uživatelů, pod kterými jsou spouštěny adaptéry CKTI a MCA nebo adresní prostor inicializátoru kanálu.
   - ID uživatelů přidružená k aplikaci pro zpracování fronty nedoručených zpráv 'special'.
3. Definujte alias frontu, která se interpretuje jako skutečná fronta nedoručených zpráv, ale přidělte alias fronty tyto atributy: PUT (ENABLED) a GET (DISABLED). Dejte alias frontě název se stejným kmenem jako název fronty nedoručených zpráv, ale připojte k tomuto kmeni znaky ". PUT". Je-li například název fronty nedoručených zpráv hlq.DEAD.QUEUE, název alias fronty bude hlq.DEAD.QUEUE.PUT.
4. Chcete-li vložit zprávu do fronty nedoručených zpráv, aplikace použije alias frontu. To je to, co musí vaše aplikace udělat:
   - Načtěte název skutečné fronty nedoručených zpráv. Za tímto účelem otevře objekt správce front pomocí příkazu MQOPEN a poté vydá příkaz MQINQ pro získání názvu fronty nedoručených zpráv.
   - Sestavte název alias fronty připojením znaků '.PUT' k tomuto názvu, v tomto případě hlq.DEAD.QUEUE.PUT.
   - Otevřete alias frontu hlq.DEAD.QUEUE.PUT.

- Vložte zprávu do skutečné fronty nedoručených zpráv zadáním příkazu MQPUT pro alias frontu.

5. Poskytněte ID uživatele přidružené k aplikaci RACF UPDATE oprávnění k aliasu, ale bez přístupu (oprávnění NONE) ke skutečné frontě nedoručených zpráv. To znamená, že:
   - Aplikace může vkládat zprávy do fronty nedoručených zpráv pomocí alias fronty.
   - Aplikace nemůže získat zprávy z fronty nedoručených zpráv pomocí alias fronty, protože alias fronta je pro operace získání zakázána.

   Aplikace nemůže získat žádné zprávy ze skutečné fronty nedoručených zpráv, protože má správné oprávnění RACF .

Tabulka 34 na stránce 206 shrnuje oprávnění RACF požadované pro různé účastníky tohoto řešení.

Tabulka 34. Oprávnění RACF pro frontu nedoručených zpráv a její alias

Přidružená ID uživatelů	**Skutečná fronta nedoručených zpráv (hlq.DEAD.QUEUE)**	**Alias fronty nedoručených zpráv (hlq.DEAD.QUEUE.PUT)**
Adresní prostor MCA nebo inicializátoru kanálu a CKTI	AKTUALIZOVAT	ŽÁDNÉ
'Speciální' aplikace (pro zpracování fronty nedoručených zpráv)	AKTUALIZOVAT	ŽÁDNÉ
ID uživatelů aplikací napsaných uživatelem	ŽÁDNÉ	AKTUALIZOVAT

Pokud použijete tuto metodu, aplikace nemůže určit maximální délku zprávy (MAXMSGL) fronty nedoručených zpráv. Je to proto, že atribut MAXMSGL nelze načíst z alias fronty. Proto by vaše aplikace měla předpokládat, že maximální délka zprávy je 100 MB, což je maximální velikost, kterou produkt IBM MQ for z/OS podporuje. Skutečná fronta nedoručených zpráv by měla být také definována s atributem MAXMSGL 100 MB.

Poznámka: Aplikační programy napsané uživatelem obvykle nepoužívají alternativní oprávnění uživatele k vložení zpráv do fronty nedoručených zpráv. Tím se sníží počet ID uživatelů, kteří mají přístup k frontě nedoručených zpráv.

z/OS *Zabezpečení systémové fronty*

Musíte nastavit přístup k produktu RACF , abyste povolili určitým ID uživatelů přístup ke konkrétním systémovým frontám.

K mnoha systémovým frontám přistupují pomocné části produktu IBM MQ:

- Obslužný program CSQUTIL
- Obslužný program zásad zabezpečení zpráv (CSQ0UTIL)
- Provozní a ovládací panely
- Adresní prostor inicializátoru kanálu (včetně démona publikování/odběru ve frontě)
- Server mqweb používaný IBM MQ Console a REST API.

ID uživatelů, pod kterými se spouští, musí mít přístup RACF k těmto frontám, jak ukazuje Tabulka 35 na stránce 207.

Tabulka 35. Přístup vyžadovaný produktem IBM MQ k frontám SYSTEM

SYSTÉMOVÁ FRONTA	CSQUTIL	CSQ0UTIL	Server mqweb	Provozní a ovládací panely	Inicializátor kanálu pro distribuované řazení do front
SYSTEM.ADMIN.CHANNEL.EVENT	-	-	-	-	AKTUALIZOVAT
SYSTEM.ADMIN.COMMAND.QUEUE	-	-	AKTUALIZOVAT	-	-
SYSTEM.BROKER.ADMIN.STREAM	-	-	-	-	ALTER
SYSTEM.BROKER.CONTROL.QUEUE	-	-	-	-	ALTER
SYSTEM.BROKER.DEFAULT.STREAM	-	-	-	-	ALTER
SYSTEM.BROKER.INTER.BROKER.COMMUNICATIONS	-	-	-	-	AKTUALIZOVAT
SYSTEM.CHANNEL.INITQ	-	-	-	-	AKTUALIZOVAT
SYSTEM.CHANNEL.SYNCQ	-	-	-	-	AKTUALIZOVAT
SYSTEM.CLUSTER.COMMAND.QUEUE	-	-	-	-	ALTER
SYSTEM.CLUSTER.REPOSITORY.QUEUE	-	-	-	-	AKTUALIZOVAT
SYSTEM.CLUSTER.TRANSMIT.QUEUE	-	-	-	-	ALTER
SYSTEM.COMMAND.INPUT	AKTUALIZOVAT	-	-	AKTUALIZOVAT	AKTUALIZOVAT
SYSTEM.COMMAND.REPLY.*	-	-	-	-	AKTUALIZOVAT
SYSTEM.COMMAND.REPLY.MODEL	AKTUALIZOVAT	-	-	AKTUALIZOVAT	AKTUALIZOVAT
SYSTEM.CSQOREXX.*	-	-	-	AKTUALIZOVAT	-
SYSTEM.CSQUTIL.*	AKTUALIZOVAT	-	-	-	-
SYSTEM.CSQXCMD.*	-	-	-	-	AKTUALIZOVAT
SYSTEM.HIERARCHY.STATE	-	-	-	-	AKTUALIZOVAT
SYSTEM.INTER.QMGR.CONTROL	-	-	-	-	AKTUALIZOVAT
SYSTEM.INTER.QMGR.PUBS	-	-	-	-	AKTUALIZOVAT
SYSTEM.INTER.QMGR.FANREQ	-	-	-	-	AKTUALIZOVAT

Tabulka 35. Přístup vyžadovaný produktem IBM MQ k frontám SYSTEM (pokračování)					
SYSTÉMOVÁ FRONTA	**CSQUTIL**	**CSQ0UTIL**	**Server mqweb**	**Provozní a ovládací panely**	**Inicializátor kanálu pro distribuované řazení do front**
SYSTEM.PROTECTION.ERROR.QUEUE	-	-	-	-	AKTUALIZOVAT
SYSTEM.PROTECTION.POLICY.QUEUE	-	Aktualizovat“1” na stránce 208	-	-	READ (čtení)
SYSTEM.QSG.CHANNEL.SYNCQ	-	-	-	-	AKTUALIZOVAT
SYSTEM.QSG.TRANSMIT.QUEUE	-	-	-	-	AKTUALIZOVAT
SYSTEM.REST.REPLY.QUEUE	-	-	AKTUALIZOVAT	-	-
SYSTEM.BLUEMIX.REGISTRATION.QUEUE	-	-	-	-	AKTUALIZOVAT

Notes:

1. Uživatel adresního prostoru Advanced Message Security také vyžaduje přístup READ k této frontě.

z/OS *Rychlý odkaz na přístup k zabezpečení prostředků rozhraní API*

Souhrn voleb **MQOPEN**, **MQPUT1**, **MQSUB**a **MQCLOSE** a přístup požadovaný různými typy zabezpečení prostředků.

Tabulka 36. Volby MQOPEN, MQPUT1, MQSUB a MQCLOSE a požadovaná bezpečnostní autorizace. Volání zobrazená podobně jako tato **(1)** naleznete v poznámkách za touto tabulkou.				
	Minimální požadovaná úroveň přístupu RACF			
RACF Třída:	**MXTOPIC**	**MQQUEUE nebo MXQUEUE (1)**	**MQADMIN nebo MXADMIN**	**MQADMIN nebo MXADMIN**
RACF Profil:	**(15 nebo 16)**	**(2)**	**(3)**	**(4)**
Volba MQOPEN				
MQOO_DOTAZOVAT		READ **(5)**	Bez kontroly	Bez kontroly
MQOO_BROWSE		READ (čtení)	Bez kontroly	Bez kontroly
MQOO_INPUT_ *		AKTUALIZOVAT	Bez kontroly	Bez kontroly
MQOO_SAVE_ALL_CONTEXT **(6)**		AKTUALIZOVAT	Bez kontroly	Bez kontroly
MQOO_OUTPUT (POUŽITÍ = NORMÁLNÍ) **(7)**		AKTUALIZOVAT	Bez kontroly	Bez kontroly

Tabulka 36. Volby MQOPEN, MQPUT1, MQSUB a MQCLOSE a požadovaná bezpečnostní autorizace. Volání zobrazená podobně jako tato **(1)** naleznete v poznámkách za touto tabulkou. *(pokračování)*

	Minimální požadovaná úroveň přístupu RACF			
RACF Třída:	**MXTOPIC**	**MQQUEUE nebo MXQUEUE (1)**	**MQADMIN nebo MXADMIN**	**MQADMIN nebo MXADMIN**
RACF Profil:	**(15 nebo 16)**	**(2)**	**(3)**	**(4)**
MQOO_PASS_IDENTITY_CONTEXT **(8)**		AKTUALIZOVAT	READ (čtení)	Bez kontroly
MQOO_PASS_ALL_CONTEXT **(8) (9)**		AKTUALIZOVAT	READ (čtení)	Bez kontroly
MQOO_SET_IDENTITY_CONTEXT **(8) (9)**		AKTUALIZOVAT	AKTUALIZOVAT	Bez kontroly
MQOO_SET_ALL_CONTEXT **(8) (10)**		AKTUALIZOVAT	CONTROL	Bez kontroly
MQOO_OUTPUT (USAGE (XMITQ) **(11)**		AKTUALIZOVAT	CONTROL	Bez kontroly
MQOO_OUTPUT (objekt tématu)	UPDATE **(16)**			
MQOO_OUTPUT (alias fronta pro objekt tématu)	UPDATE **(16)**	AKTUALIZOVAT		
MQOO_SET		ALTER	Bez kontroly	Bez kontroly
Oprávnění MQOO_ALTERNATE_USER_AUTHORITY		**(12)**	**(12)**	AKTUALIZOVAT
Volba MQPUT1				
Vložit do normální fronty **(7)**		AKTUALIZOVAT	Bez kontroly	Bez kontroly
MQPMO_PASS_IDENTITY_CONTEXT		AKTUALIZOVAT	READ (čtení)	Bez kontroly
MQPMO_PASS_ALL_CONTEXT		AKTUALIZOVAT	READ (čtení)	Bez kontroly
MQPMO_SET_IDENTITY_CONTEXT		AKTUALIZOVAT	AKTUALIZOVAT	Bez kontroly
MQPMO_SET_ALL_CONTEXT		AKTUALIZOVAT	CONTROL	Bez kontroly
MQOO_OUTPUT Vložit do přenosové fronty **(11)**		AKTUALIZOVAT	CONTROL	Bez kontroly
MQOO_OUTPUT (objekt tématu)	UPDATE **(16)**			
MQOO_OUTPUT (alias fronta pro objekt tématu)	UPDATE **(16)**	AKTUALIZOVAT		
Oprávnění MQPMO_ALTERNATE_USER_AUTHORITY		**(13)**	**(13)**	AKTUALIZOVAT
Volba MQCLOSE				

Tabulka 36. Volby MQOPEN, MQPUT1, MQSUB a MQCLOSE a požadovaná bezpečnostní autorizace. Volání zobrazená podobně jako tato **(1)** naleznete v poznámkách za touto tabulkou. *(pokračování)*				
	Minimální požadovaná úroveň přístupu RACF			
RACF Třída:	**MXTOPIC**	**MQQUEUE nebo MXQUEUE (1)**	**MQADMIN nebo MXADMIN**	**MQADMIN nebo MXADMIN**
RACF Profil:	**(15 nebo 16)**	**(2)**	**(3)**	**(4)**
MQCO_DELETE **(14)**		ALTER	Bez kontroly	Bez kontroly
MQCO_DELETE_PURGE **(14)**		ALTER	Bez kontroly	Bez kontroly
MQCO_REMOVE_SUB	ALTER **(15)**			
Volba MQSUB				
MQSO_CREATE	ALTER **(15)**	**(17)**	**(18)**	
MQSO_ALTER	ALTER **(15)**	**(17)**	**(18)**	
MQSO_RESUME	READ **(15)**	**(17)**	Bez kontroly	
MQSO_ALTERNATE_USER_AUTHORITY				AKTUALIZOVAT
MQSO_SET_IDENTITY_CONTEXT			**(18)**	

Poznámka:

1. Tato volba není omezena na fronty. Pro seznamy názvů použijte třídu MQNLIST nebo MXNLIST a pro procesy třídu MQPROC nebo MXPROC.
2. Použijte profil RACF : hlq.resourcename
3. Použijte profil RACF : hlq.CONTEXT.queuename
4. Použijte profil RACF : hlq.ALTERNATE.USER. `alternateuserid`

   `alternateuserid` je identifikátor uživatele, který je uveden v poli *`AlternateUserId`* deskriptoru objektu. Všimněte si, že pro tuto kontrolu se použije až 12 znaků pole *`AlternateUserId`* , na rozdíl od ostatních kontrol, kde se používá pouze prvních 8 znaků identifikátoru uživatele.
5. Při otevírání správce front pro dotazy se neprovádí žádná kontrola.
6. Také musí být zadána hodnota MQOO_INPUT_ *. Toto je platné pro lokální, modelovou nebo alias frontu.
7. Tato kontrola se provádí pro lokální nebo modelovou frontu, která má atribut fronty **Usage** MQUS_NORMAL, a také pro alias nebo vzdálenou frontu (která je definována pro připojeného správce front). Pokud se jedná o vzdálenou frontu, která je otevřena, s uvedením *`ObjectQMgrName`* (nikoli názvu připojeného správce front) explicitně, kontrola se provede pro frontu se stejným názvem jako *`ObjectQMgrName`* (což musí být lokální fronta s atributem fronty **Usage** MQUS_TRANSMISSION).
8. Musí být uveden také parametr MQOO_OUTPUT.
9. MQOO_PASS_IDENTITY_CONTEXT je také odvozen z této volby.
10. MQOO_PASS_IDENTITY_CONTEXT, MQOO_PASS_ALL_CONTEXT a MQOO_SET_IDENTITY_CONTEXT jsou také odvozeny z této volby.
11. Tato kontrola se provádí pro lokální nebo modelovou frontu, která má atribut fronty **Usage** MQUS_TRANSMISSION a otevírá se přímo pro výstup. Nepoužije se, pokud se otevírá vzdálená fronta.
12. Musí být zadán také alespoň jeden z parametrů MQOOO_INQUIRE, MQOO_BROWSE, MQOO_INPUT_ *, MQOO_OUTPUT nebo MQOO_SET. Provedená kontrola je stejná jako u ostatních uvedených voleb.
13. Provedená kontrola je stejná jako u ostatních uvedených voleb.

14. To platí pouze pro trvalé dynamické fronty, které byly otevřeny přímo, tj. nebyly otevřeny prostřednictvím modelové fronty. K odstranění dočasné dynamické fronty není vyžadováno žádné zabezpečení.
15. Použijte RACF profile hlq.SUBSCRIBE.topicname.
16. Použijte RACF profil hlq.PUBLISH.topicname.
17. Pokud jste v požadavku MQSUB zadali cílovou frontu pro publikování, do které má být odesláno, provede se kontrola zabezpečení pro tuto frontu, aby se zajistilo, že máte k této frontě oprávnění.
18. Pokud chcete v požadavku MQSUB s určenými volbami MQSO_CREATE nebo MQSO_ALTER nastavit libovolné pole kontextu identity ve struktuře MQSD, musíte také zadat volbu MQSO_SET_IDENTITY_CONTEXT a také potřebujete příslušné oprávnění pro profil kontextu pro cílovou frontu.

z/OS *Profily pro zabezpečení témat*

Je-li aktivní zabezpečení tématu, musíte definovat profily v příslušných třídách a povolit potřebné skupiny nebo ID uživatelů přístup k těmto profilům.

Koncepce zabezpečení témat v rámci stromu témat je popsána v tématu Zabezpečení publikování/odběru.

Je-li zabezpečení tématu aktivní, musíte provést následující akce:

- Definujte profily ve třídách **MXTOPIC** nebo **GMXTOPIC** .
- Povolte nezbytné skupiny nebo ID uživatelů přístup k těmto profilům, aby mohli vydávat požadavky rozhraní IBM MQ API, které používají témata.

Profily pro zabezpečení témat jsou ve tvaru:

```
hlq.SUBSCRIBE.topicname
hlq.PUBLISH.topicname
```

kde:

- `hlq` je buď `qmgr-name` (název správce front), nebo `qsg-name` (název skupiny sdílení front).
- `topicname` je název uzlu administrace témat ve stromu témat, který je přidružen buď k tématu přihlášenému k odběru prostřednictvím volání MQSUB, nebo k publikování prostřednictvím volání MQOPEN.

Profil s předponou názvu správce front řídí přístup k jednomu tématu v daném správci front. Profil s předponou názvu skupiny sdílení front řídí přístup k jednomu nebo více tématům s daným názvem tématu ve všech správcích front v rámci skupiny sdílení front. Tento přístup lze v jednotlivých správcích front potlačit definováním profilu úrovně správce front pro dané téma v daném správci front.

Pokud je váš správce front členem skupiny sdílení front a používáte zabezpečení na úrovni správce front i skupiny sdílení front, produkt IBM MQ nejprve zkontroluje profil s předponou podle názvu správce front. Pokud jej nenajde, vyhledá profil s předponou názvu skupiny sdílení front.

Odebírat

Chcete-li se přihlásit k odběru tématu, potřebujete přístup jak k tématu, ke kterému se pokoušíte přihlásit, tak k cílové frontě pro publikování.

Když zadáte požadavek MQSUB, budou provedeny následující kontroly zabezpečení:

- Zda máte odpovídající úroveň přístupu pro přihlášení k odběru daného tématu a také zda je pro výstup otevřena cílová fronta (je-li zadána).
- Zda máte odpovídající úroveň přístupu k dané cílové frontě.

Tabulka 37. Úroveň přístupu požadovaná pro přihlášení k odběru zabezpečení tématu	
Volba MQSUB	**RACF požadovaný přístup k profilu `hlq.SUBSCRIBE.topicname` ve třídě MXTOPIC**
MQSO_CREATE a MQSO_ALTER	ALTER
MQSO_RESUME	READ (čtení)

Tabulka 38. Pro přihlášení k odběru s použitím nespravované cílové fronty je vyžadováno další oprávnění.	
Volba MQSUB	**RACF požadovaný přístup k profilu `hlq.CONTEXT.queuename` ve třídě MQADMIN nebo MXADMIN**
MQSO_CREATE, MQSO_ALTER a MQSO_RESUME	AKTUALIZOVAT
	RACF požadovaný přístup k profilu `hlq.queuename` ve třídě MQQUEUE nebo MXQUEUE
MQSO_CREATE a MQSO_ALTER	AKTUALIZOVAT
	RACF požadovaný přístup k profilu `hlq.ALTERNATE.USER.alternateuserid` ve třídě MQADMIN nebo MXADMIN
MQSO_ALTERNATE_USER_AUTHORITY	AKTUALIZOVAT

Aspekty spravovaných front pro odběry

Provede se kontrola zabezpečení, abyste zjistili, zda máte povoleno přihlásit se k odběru tématu. Při vytvoření spravované fronty se však neprovádějí žádné kontroly zabezpečení nebo se zjišťuje, zda máte přístup ke vkládaným zprávám do této cílové fronty.

Nelze zavřít odstranění spravované fronty.

Použité modelové fronty jsou: `SYSTEM.DURABLE.MODEL.QUEUE` a `SYSTEM.NDURABLE.MODEL.QUEUE`.

Spravované fronty vytvořené z těchto modelových front jsou ve tvaru `SYSTEM.MANAGED.DURABLE.A346EF00367849A0` a `SYSTEM.MANAGED.NDURABLE.A346EF0036785EA0` , kde je poslední kvalifikátor nepředvídatelný.

Neudělejte uživateli přístup k těmto frontám. Fronty lze chránit pomocí generických profilů formuláře `SYSTEM.MANAGED.DURABLE.*` a `SYSTEM.MANAGED.NDURABLE.*` bez udělených oprávnění.

Zprávy lze načíst z těchto front pomocí popisovače vráceného v požadavku MQSUB.

Pokud explicitně zadáte volání MQCLOSE pro odběr se zadanou volbou `MQCO_REMOVE_SUB` a nevytvořili jste odběr, který zavíráte pod tímto popisovačem, provede se v době uzavření kontrola zabezpečení, abyste se ujistili, že máte správné oprávnění k provedení operace.

Tabulka 39. Úroveň přístupu vyžadovaná pro profily pro zabezpečení tématu pro uzavření operace odběru	
Volba MQCLOSE	**RACF požadovaný přístup k profilu `hlq.SUBSCRIBE.topicname` ve třídě MXTOPIC**
MQCO_REMOVE_SUB	ALTER

Publikovat

Chcete-li publikovat na téma, potřebujete přístup k tématu, a pokud používáte alias fronty, také k alias frontě.

Tabulka 40. Úroveň přístupu požadovaná pro publikování zabezpečení tématu	
Volba MQOPEN nebo MQPUT1	**RACF požadovaný přístup k profilu `hlq.PUBLISH.topicname` ve třídě MXTOPIC**
MQOO_OUTPUT nebo MQPUT1	AKTUALIZOVAT

Tabulka 41. Úroveň přístupu potřebná k otevření alias fronty, která se interpretuje jako téma	
Volba MQOPEN nebo MQPUT1	**RACF požadovaný přístup k profilu `hlq.queuename` ve třídě MQQUEUE nebo MXQUEUE pro alias frontu**
MQOO_OUTPUT nebo MQPUT1	AKTUALIZOVAT

Podrobnosti o tom, jak funguje zabezpečení tématu, když je pro publikování otevřena alias fronta, která se interpretuje jako název tématu, viz “Aspekty pro fronty aliasů, které se interpretují na témata pro operaci publikování” na stránce 213.

Pokud uvážíte alias fronty použité pro cílové fronty pro omezení PUT nebo GET, prohlédněte si téma “Aspekty pro fronty aliasů” na stránce 202.

Pokud se změní úroveň přístupu RACF , kterou má aplikace k profilu zabezpečení tématu, projeví se změny pouze pro všechny nově získané manipulátory objektů (tj. pro nové MQSUB nebo MQOPEN) pro dané téma. Tyto popisovače, které již existovaly v době změny, si zachovávají svůj stávající přístup k tématu. Stávající odběratelé si také zachovávají přístup k předplatitelům, které již provedli.

Aspekty pro fronty aliasů, které se interpretují na témata pro operaci publikování

Když zadáte volání MQOPEN nebo MQPUT1 pro alias frontu, která se interpretuje na téma, produkt IBM MQ provede dvě kontroly prostředků:

- První pro název alias fronty určený v deskriptoru objektu (MQOD) ve volání MQOPEN nebo MQPUT1 .
- Druhá pro téma, na které se interpretuje alias fronta

Musíte si uvědomit, že toto chování se liší od chování, které získáte, když se alias fronty interpretují na jiné fronty. Chcete-li pokračovat v akci publikování, potřebujete správný přístup k oběma profilům.

Zabezpečení tématu systému

K následujícím systémovým tématům přistupuje adresní prostor inicializátoru kanálu.

ID uživatelů, pod kterými se toto spouští, musí mít RACF přístup k těmto frontám, jak ukazuje Tabulka 42 na stránce 213.

Tabulka 42. Vyžadovaný přístup k tématům SYSTEM		
Téma SYSTEM	**Profil**	**Inicializátor kanálu pro distribuované řazení do front**
SYSTEM.BROKER.ADMIN.STREAM	hlq.PUBLISH.topicname	AKTUALIZOVAT
SYSTEM.BROKER.ADMIN.STREAM	hlq.SUBSCRIBE.topicname	ALTER

z/OS *Profily pro procesy*

Je-li aktivní zabezpečení procesu, musíte definovat profily v příslušných třídách a povolit potřebné skupiny nebo ID uživatelů přístup k těmto profilům.

Je-li zabezpečení procesu aktivní, musíte:

- Definujte profily ve třídách **MQPROC** nebo **GMQPROC** , používáte-li profily s velkými písmeny.

- Definujte profily ve třídách **MXPROC** nebo **GMXPROC** , pokud používáte profily se smíšenými velkými a velkými písmeny.
- Povolte potřebné skupiny nebo ID uživatelů přístup k těmto profilům, aby mohli vydávat požadavky rozhraní IBM MQ API, které používají procesy.

Profily pro procesy jsou ve formě:

```
hlq.processname
```

kde `hlq` může být buď `qmgr-name` (název správce front), nebo `qsg-name` (název skupiny sdílení front) a `processname` je název otevíraného procesu.

Profil s předponou názvu správce front řídí přístup k jedné definici procesu v daném správci front. Profil s předponou názvu skupiny sdílení front řídí přístup k jedné nebo více definicím procesů s tímto názvem ve všech správcích front v rámci skupiny sdílení front. Tento přístup lze v jednotlivých správcích front potlačit definováním profilu úrovně správce front pro danou definici procesu v daném správci front.

Pokud je váš správce front členem skupiny sdílení front a používáte zabezpečení na úrovni správce front i skupiny sdílení front, produkt IBM MQ nejprve zkontroluje profil s předponou podle názvu správce front. Pokud jej nenajde, vyhledá profil s předponou názvu skupiny sdílení front.

Následující tabulka zobrazuje přístup nezbytný pro otevření procesu.

Tabulka 43. Úrovně přístupu pro zabezpečení procesu

Volba MQOPEN	**RACF úroveň přístupu požadovaná pro hlq.processname**
MQOO_DOTAZOVAT	READ (čtení)

Například ve správci front MQS9musí být skupina RACF INQVPRC schopna provést dotaz (`MQINQ`). u všech procesů začínajících písmenem V. Definice RACF pro toto by byly:

```
RDEFINE MQPROC MQS9.V* UACC(NONE)
PERMIT MQS9.V* CLASS(MQPROC) ID(INQVPRC) ACCESS(READ)
```

V závislosti na otevřených volbách zadaných při otevření objektu definice procesu může být aktivní také alternativní zabezpečení uživatele.

z/OS *Profily pro seznamy názvů*

Pokud je aktivní zabezpečení seznamu názvů, definujte profily v příslušných třídách a poskytněte potřebným skupinám nebo ID uživatelů přístup k těmto profilům.

Pokud je aktivní zabezpečení seznamu názvů, musíte:

- Definujte profily ve třídách **MQNLIST** nebo **GMQNLIST** , používáte-li profily s velkými písmeny.
- Definujte profily ve třídách **MXNLIST** nebo **GMXNLIST** , pokud používáte profily se smíšenými velkými a velkými písmeny.
- Povolte potřebné skupiny nebo ID uživatelů přístup k těmto profilům.

Profily pro seznamy názvů jsou ve tvaru:

```
hlq.namelistname
```

kde `hlq` může být buď `qmgr-name` (název správce front), nebo `qsg-name` (název skupiny sdílení front) a `namelistname` je název otevíraného seznamu názvů.

Profil s předponou názvu správce front řídí přístup k jednomu seznamu názvů v daném správci front. Profil s předponou názvu skupiny sdílení front řídí přístup k jednomu nebo více seznamům názvů s tímto názvem ve všech správcích front v rámci skupiny sdílení front. Tento přístup lze v jednotlivých správcích front potlačit definováním profilu na úrovni správce front pro daný seznam názvů v daném správci front.

Pokud je váš správce front členem skupiny sdílení front a používáte zabezpečení na úrovni správce front i skupiny sdílení front, produkt IBM MQ nejprve zkontroluje profil s předponou podle názvu správce front. Pokud jej nenajde, vyhledá profil s předponou názvu skupiny sdílení front.

Následující tabulka zobrazuje přístup nezbytný pro otevření seznamu názvů.

Tabulka 44. Úrovně přístupu pro zabezpečení seznamu názvů

Volba MQOPEN	**RACF úroveň přístupu požadovaná pro hlq.namelistname**
MQOO_DOTAZOVAT	READ (čtení)

Například ve správci front (nebo ve skupině sdílení front) PQM3musí být RACF skupina DEPT571 schopna se dotazovat (`MQINQ`) na těchto seznamech jmen:

- Všechny seznamy názvů začínající na "DEPT571".
- PRINTER/DESTINATIONS/DEPT571
- AGENCY/REQUEST/QUEUES (požadování/fronty)
- WAREHOUSE.BROADCAST

Definice RACF , které to mají provést, jsou:

```
RDEFINE MQNLIST PQM3.DEPT571.** UACC(NONE)
PERMIT PQM3.DEPT571.** CLASS(MQNLIST) ID(DEPT571) ACCESS(READ)

RDEFINE GMQNLIST NLISTS.FOR.DEPT571 UACC(NONE)
        ADDMEM(PQM3.PRINTER/DESTINATIONS/DEPT571,
               PQM3.AGENCY/REQUEST/QUEUES,
               PQM3.WAREHOUSE.BROADCAST)
PERMIT NLISTS.FOR.DEPT571 CLASS(GMQNLIST) ID(DEPT571) ACCESS(READ)
```

V závislosti na volbách zadaných při otevření objektu seznamu názvů může být aktivní alternativní zabezpečení uživatele.

Zabezpečení seznamu názvů systému

K mnoha systémovým seznamům názvů přistupují pomocné části produktu IBM MQ:

- Obslužný program CSQUTIL
- Provozní a ovládací panely
- Adresní prostor inicializátoru kanálu (včetně démona publikování/odběru zařazeného ve frontě)

ID uživatelů, pod kterými se tyto seznamy spouštějí, musí mít přístup RACF k těmto seznamům názvů, jak je uvedeno v části Tabulka 45 na stránce 215.

Tabulka 45. Přístup vyžadovaný k seznamům názvů SYSTEM pomocí IBM MQ

Seznam názvů SYSTEM	**CSQUTIL**	**Provozní a ovládací panely**	**Inicializátor kanálu pro distribuované řazení do front**
SYSTEM.QPUBSUB.QUEUE.NAMELIST	-	-	READ (čtení)
SYSTEM.QPUBSUB.SUBPOINT.NAMELIST	-	-	READ (čtení)

z/OS *Profily pro alternativní zabezpečení uživatele*

Je-li aktivní alternativní zabezpečení uživatele, musíte definovat profily v odpovídajících třídách a povolit potřebné skupiny nebo ID uživatelů přístup k těmto profilům.

Další informace o produktu *AlternateUserId*naleznete v tématu AlternateUser(MQCHAR12).

Je-li aktivní alternativní zabezpečení uživatele, musíte:

- Pokud používáte profily s velkými písmeny, definujte profily ve třídách MQADMIN nebo GMQADMIN.
- Definujte profily ve třídách MXADMIN nebo GMXADMIN, pokud používáte profily smíšených případů.

Povolte potřebné skupiny nebo ID uživatelů přístup k těmto profilům, aby mohli při otevření objektu používat volby ALTERNATE_USER_AUTHORITY.

Profily pro alternativní zabezpečení uživatele lze zadat na úrovni subsystému nebo na úrovni skupiny sdílení front a mají následující podobu:

```
hlq.ALTERNATE.USER.alternateuserid
```

Kde `hlq` může být buď `qmgr-name` (název správce front), nebo `qsg-name` (název skupiny sdílení front) a `alternateuserid` je hodnota pole *AlternateUserId* v deskriptoru objektu.

Profil s předponou názvu správce front řídí použití alternativního ID uživatele v daném správci front. Profil s předponou názvu skupiny sdílení front řídí použití alternativního ID uživatele ve všech správcích front v rámci skupiny sdílení front. Toto alternativní ID uživatele lze použít v libovolném správci front v rámci skupiny sdílení front uživatelem, který má správný přístup. Tento přístup lze v jednotlivých správcích front potlačit definováním profilu úrovně správce front pro příslušné alternativní ID uživatele v daném správci front.

Pokud je váš správce front členem skupiny sdílení front a používáte zabezpečení na úrovni správce front i skupiny sdílení front, produkt IBM MQ nejprve zkontroluje profil s předponou podle názvu správce front. Pokud jej nenajde, vyhledá profil s předponou názvu skupiny sdílení front.

Následující tabulka zobrazuje přístup při zadávání alternativní volby uživatele.

Tabulka 46. Úrovně přístupu pro alternativní zabezpečení uživatele

MQOPEN, MQSUB nebo volba MQPUT1	**RACF požadovaná úroveň přístupu**
MQOO_ALTERNATE_USER_AUTHORITY MQSO_ALTERNATE_USER_AUTHORITY MQPMO_ALTERNATE_USER_AUTHORITY	AKTUALIZOVAT

Kromě alternativních kontrol zabezpečení uživatelů lze také provádět další kontroly zabezpečení pro zabezpečení front, procesů, seznamů názvů a kontextů. Alternativní ID uživatele, je-li poskytnuto, se používá pouze pro kontroly zabezpečení u prostředků fronty, definice procesu nebo seznamu názvů. V případě kontrol zabezpečení alternativního uživatele a kontextu se použije ID uživatele požadující kontrolu. Podrobnosti o způsobu zpracování ID uživatelů viz “ID uživatelů pro kontrolu zabezpečení na systému z/OS” na stránce 239. Chcete-li zobrazit souhrnnou tabulku zobrazující volby otevření a kontroly zabezpečení vyžadované v případě, že je aktivní zabezpečení fronty, kontextu a alternativního uživatele, prohlédněte si téma Tabulka 36 na stránce 208.

Alternativní profil uživatele poskytuje požadujícímu ID uživatele přístup k prostředkům přidruženým k ID uživatele uvedenému v alternativním ID uživatele. Například mzdový server spuštěný pod ID uživatele PAYSERV ve správci front QMPY zpracovává požadavky od ID uživatelů personálu, z nichž všechny začínají na PS. K tomu, aby práce provedená mzdovým serverem byla provedena pod ID uživatele požadujícího uživatele, použije se alternativní oprávnění uživatele. Mzdový server ví, které ID uživatele zadat jako alternativní ID uživatele, protože požadující programy generují zprávy pomocí volby vložení zprávy MQPMO_DEFAULT_CONTEXT. Další podrobnosti o tom, odkud jsou získána alternativní ID uživatelů, naleznete v části “ID uživatelů pro kontrolu zabezpečení na systému z/OS” na stránce 239 .

Následující příklady definic RACF umožňují programu serveru zadat alternativní ID uživatelů začínající znaky PS:

```
RDEFINE MQADMIN QMPY.ALTERNATE.USER.PS* UACC(NONE)
PERMIT QMPY.ALTERNATE.USER.PS* CLASS(MQADMIN) ID(PAYSERV) ACCESS(UPDATE)
```

Poznámka:

1. Pole *AlternateUserId* v deskriptoru objektu a deskriptoru odběru jsou dlouhá 12 bajtů. Všech 12 bajtů se použije v kontrolách profilu, ale pouze prvních 8 bajtů se použije jako ID uživatele pro IBM MQ. Není-li toto zkrácení ID uživatele žádoucí, musí aplikační programy provádějící požadavek převést jakékoli alternativní ID uživatele přes 8 bajtů na něco vhodnějšího.
2. Pokud zadáte volby MQOOO_ALTERNATE_USER_AUTHORITY, MQSO_ALTERNATE_USER_AUTHORITY nebo MQPMO_ALTERNATE_USER_AUTHORITY a neuvedete pole *AlternateUserId* v deskriptoru objektu, použije se ID uživatele s mezerami. Pro účely alternativního zabezpečení uživatele zkontrolujte, že ID uživatele použité pro kvalifikátor *AlternateUserId* je -BLANK-. Například RDEF MQADMIN hlq.ALTERNATE.USER.-BLANK-.

   Pokud má uživatel povolen přístup k tomuto profilu, všechny další kontroly se provádějí s ID uživatele s mezerami. Podrobnosti o prázdných ID uživatelů viz "Prázdná ID uživatelů a úrovně UACC" na stránce 247.

Administrace alternativních ID uživatelů je jednodušší, pokud máte konvenci pojmenování pro ID uživatelů, která vám umožňuje používat generické alternativní profily uživatelů. Pokud ne, můžete použít funkci RACF RACVAR. Podrobnosti o použití RACVAR naleznete v dokumentaci k produktu z/OS Security Server RACF .

Při vložení zprávy do fronty, která byla otevřena s alternativním oprávněním uživatele, a při vygenerování kontextu zprávy správcem front je pole MQMD_USER_IDENTIFIER nastaveno na alternativní ID uživatele.

z/OS *Profily pro zabezpečení kontextu*

Je-li aktivní zabezpečení kontextu, musíte pro řízení přístupu k informacím o kontextu zprávy definovat profily v příslušných třídách a povolit potřebné skupiny nebo ID uživatelů přístup k těmto profilům. Kontext zprávy je obsažen v deskriptoru zprávy (MQMD).

Použití profilů pro zabezpečení kontextu

Je-li aktivní zabezpečení kontextu, musíte uživatelům povolit přístup k informacím o kontextu pro zprávy v konkrétní frontě nebo při publikování do konkrétního tématu definovat profil v jedné z následujících tříd:

- Třída MQADMIN , používáte-li profily s velkými písmeny.
- Třída MXADMIN , používáte-li profily se smíšenými velkými a velkými písmeny.

Profily pro zabezpečení kontextu lze určit na úrovni subsystému nebo na úrovni skupiny sdílení front a mají následující podobu:

```
hlq.CONTEXT.queuename
hlq.CONTEXT.topicname
```

kde *hlq* může být buď název správce front, nebo název skupiny sdílení front, a *queuename* a *topicname* může být buď úplný, nebo generický název fronty nebo tématu, pro které chcete definovat profil kontextu.

Profil s předponou názvu správce front a s názvem ** zadaným jako název fronty nebo tématu umožňuje řízení zabezpečení kontextu ve všech frontách a tématech náležejících danému správci front. Toto nastavení lze přepsat pro jednotlivou frontu nebo téma definováním specifického profilu pro kontext v dané frontě nebo tématu.

Profil s předponou názvu skupiny sdílení front a s názvem ** zadaným jako název fronty nebo tématu umožňuje řízení kontextu ve všech frontách a tématech náležejících správcům front v rámci skupiny sdílení front. Tuto hodnotu lze v jednotlivých správcích front potlačit definováním profilu na úrovni správce

front pro kontext v daném správci front zadáním profilu s předponou s názvem správce front. Může být také přepsán pro jednotlivou frontu nebo téma zadáním profilu s příponou názvu fronty nebo tématu.

Pokud je váš správce front členem skupiny sdílení front a používáte zabezpečení na úrovni správce front i skupiny sdílení front, produkt IBM MQ nejprve zkontroluje profil s předponou podle názvu správce front. Pokud jej nenajde, vyhledá profil s předponou názvu skupiny sdílení front.

Musíte povolit nezbytné skupiny nebo ID uživatelů přístup k tomuto profilu. Následující tabulka zobrazuje požadovanou úroveň přístupu v závislosti na specifikaci voleb kontextu při otevření fronty.

Tabulka 47. Úrovně přístupu pro zabezpečení kontextu

Volba MQOPEN nebo MQPUT1	**RACF úroveň přístupu požadovaná pro hlq.CONTEXT.queuename nebo hlq.CONTEXT.topicname**
MQPMO_NO_CONTEXT	Žádná kontrola zabezpečení kontextu
MQPMO_DEFAULT_CONTEXT	Žádná kontrola zabezpečení kontextu
MQOO_SAVE_ALL_CONTEXT	Žádná kontrola zabezpečení kontextu
MQOO_PASS_IDENTITY_CONTEXT MQPMO_PASS_IDENTITY_CONTEXT	READ (čtení)
MQOO_PASS_ALL_CONTEXT MQPMO_PASS_ALL_CONTEXT	READ (čtení)
MQOO_SET_IDENTITY_CONTEXT MQPMO_SET_IDENTITY_CONTEXT	AKTUALIZOVAT
MQOO_SET_ALL_CONTEXT MQPMO_SET_ALL_CONTEXT	CONTROL
MQOO_OUTPUT nebo MQPUT1(USAGE (XMITQ))	CONTROL
Volba MQSUB	
MQSO_SET_IDENTITY_CONTEXT **(Poznámka 2)**	AKTUALIZOVAT

Poznámka:

1. ID uživatelů používaná pro distribuované fronty vyžadují přístup `CONTROL` k produktu `hlq.CONTEXT.queuename` pro vložení zpráv do cílové fronty. Informace o použitých ID uživatelů viz “ID uživatelů používaná inicializátorem kanálu” na stránce 242 .
2. Pokud chcete v požadavku MQSUB s určenými volbami `MQSO_CREATE` nebo `MQSO_ALTER` nastavit libovolné pole kontextu identity ve struktuře MQSD, musíte zadat volbu `MQSO_SET_IDENTITY_CONTEXT` . Požadujete také odpovídající oprávnění ke kontextovým profilům pro cílovou frontu.

Pokud vložíte příkazy do vstupní fronty systémových příkazů, použijte výchozí volbu kontextové vložení zprávy pro přidružení správného ID uživatele k příkazu.

Například obslužný program CSQUTIL dodávaný s produktem IBM MQlze použít k odlehčování a opětnému načítání zpráv ve frontách. Při obnově odlehčených zpráv do fronty obslužný program CSQUTIL pomocí volby `MQOO_SET_ALL_CONTEXT` vrátí zprávy do původního stavu. Kromě zabezpečení fronty vyžadované touto volbou otevření je vyžadováno také oprávnění kontextu. Je-li například toto oprávnění vyžadováno skupinou BACKGRP ve správci front MQS1, bude definováno takto:

```
RDEFINE MQADMIN MQS1.CONTEXT.** UACC(NONE)
PERMIT MQS1.CONTEXT.** CLASS(MQADMIN) ID(BACKGRP) ACCESS(CONTROL)
```

V závislosti na zadaných volbách a typech provedeného zabezpečení se mohou při otevření fronty vyskytnout i jiné typy kontrol zabezpečení. Mezi ně patří zabezpečení fronty (viz “Profily pro zabezpečení

fronty” na stránce 200) a alternativní zabezpečení uživatele (viz “Profily pro alternativní zabezpečení uživatele” na stránce 216). Chcete-li zobrazit souhrnnou tabulku zobrazující volby otevření a kontroly zabezpečení vyžadované v případě, že je aktivní zabezpečení fronty, kontextu a alternativního uživatele, prohlédněte si téma Tabulka 36 na stránce 208.

Zabezpečení kontextu systémové fronty

K mnoha systémovým frontám přistupují pomocné části produktu IBM MQ, například adresní prostor inicializátoru kanálu, a server mqweb používaný aplikacemi IBM MQ Console a REST API.

ID uživatelů, pod nimiž jsou spouštěny, musí mít přístup RACF k těmto frontám, jak ukazuje Tabulka 48 na stránce 219.

Tabulka 48. Pro kontextové operace je vyžadován přístup k frontám SYSTEM.

SYSTÉMOVÁ FRONTA	Inicializátor kanálu pro distribuované řazení do front	Server mqweb
SYSTEM.ADMIN.COMMAND.QUEUE	-	CONTROL
SYSTEM.BROKER.CONTROL.QUEUE	CONTROL	-
SYSTEM.BROKER.INTER.BROKER.COMMUNICATIONS	CONTROL	-
SYSTEM.CHANNEL.SYNCQ	CONTROL	-
SYSTEM.CLUSTER.COMMAND.QUEUE	CONTROL	-
SYSTEM.CLUSTER.TRANSMIT.QUEUE	CONTROL	-

z/OS *Profily pro zabezpečení příkazů*

Chcete-li povolit kontrolu zabezpečení pro příkazy, přidejte profily do třídy MQCMDS. Názvy profilů jsou založeny na příkazech MQSC, ale řídí příkazy MQSC i PCF. Profily lze použít pro správce front nebo pro skupinu sdílení front.

Pokud chcete kontrolu zabezpečení pro příkazy (takže jste nedefinovali profil přepínače zabezpečení příkazu hlq.NO.CMD.CHECKS) musíte přidat profily do třídy MQCMDS.

Stejné profily zabezpečení řídí příkazy MQSC i PCF. Názvy profilů RACF pro kontrolu zabezpečení příkazů jsou založeny na samotných názvech příkazů MQSC. Tyto profily mají formu:

```
hlq.verb.pkw
```

Kde `hlq` může být buď `qmgr-name` (název správce front), nebo `qsg-name` (název skupiny sdílení front), `verb` je slovesná část názvu příkazu, například ALTER, a `pkw` je typ objektu, například QLOCAL pro lokální frontu.

Název profilu pro příkaz ALTER QLOCAL v subsystému CSQ1 je tedy následující:

```
CSQ1.ALTER.QLOCAL
```

Generické profily můžete použít k ochraně sad příkazů, abyste měli méně profilů k údržbě, a tedy méně seznamů pro přístup. Zvažte vytvoření generického profilu, který se vztahuje na všechny příkazy, které nejsou chráněny specifičtějším profilem. Definujte tento profil s UACC (NONE) a udělte přístup ALTER pouze skupinám RACF , které obsahují administrátory. Pak můžete vytvořit generický profil použitelný pro všechny příkazy DISPLAY a udělit k němu rozšířený přístup. Mezi těmito extrémy můžete identifikovat skupiny uživatelů, kteří potřebují přístup k určitým sadám příkazů. V takovém případě můžete vytvořit profily pro tyto sady a udělit přístup skupinám RACF , které představují tyto třídy uživatelů. Vyhněte se tomu, aby měli uživatelé přístup k příkazům, které nevyžadují: Použijte zásadu nejmenšího oprávnění, aby měli uživatelé přístup pouze k příkazům, které jsou vyžadovány pro jejich úlohy.

Použití příkazu v tomto správci front řídí profil s předponou názvu správce front. Profil s předponou názvu skupiny sdílení front řídí použití příkazu ve všech správcích front v rámci skupiny sdílení front. Tento přístup lze v jednotlivých správcích front potlačit definováním profilu úrovně správce front pro daný příkaz v daném správci front.

Pokud je váš správce front členem skupiny sdílení front a používáte zabezpečení na úrovni správce front i skupiny sdílení front, produkt IBM MQ zkontroluje profil s předponou podle názvu správce front. Pokud jej nenajde, vyhledá profil s předponou názvu skupiny sdílení front.

Nastavením profilů příkazů na úrovni správce front lze uživateli omezit zadávání příkazů v konkrétním správci front. Alternativně můžete definovat jeden profil pro skupinu sdílení front pro každé příkazové slovo a všechny kontroly zabezpečení pro tento profil se provádějí namísto jednotlivých správců front.

Pokud je aktivní zabezpečení subsystému i zabezpečení skupiny sdílení front a lokální profil není nalezen, provede se kontrola zabezpečení příkazu, aby se zjistilo, zda má uživatel přístup k profilu skupiny sdílení front.

Použijete-li atribut CMDSCOPE ke směrování příkazu na jiné správce front ve skupině sdílení front, bude kontrolováno zabezpečení pro každého správce front, v němž je příkaz spuštěn, nikoli však nutně pro správce front, v němž je příkaz zadán.

V tabulce Tabulka 49 na stránce 220 jsou pro každý příkaz produktu IBM MQ MQSC uvedeny profily vyžadované pro provedení kontroly zabezpečení příkazu a odpovídající úroveň přístupu pro každý profil ve třídě MQCMDS.

V tabulce Tabulka 50 na stránce 226 jsou pro každý příkaz produktu IBM MQ PCF uvedeny profily vyžadované pro provedení kontroly zabezpečení příkazu a odpovídající úroveň přístupu pro každý profil ve třídě MQCMDS.

Tabulka 49. Příkazy MQSC, profily a jejich úrovně přístupu

Příkaz	**Profil příkazu pro MQCMDS**	**Úroveň přístupu pro MQCMDS**	**Profil prostředku příkazu pro MQADMIN nebo MXADMIN**	**Úroveň přístupu pro MQADMIN nebo MXADMIN**
ALTER AUTHINFO	hlq.ALTER.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
POZMĚNIT FOND VYROVNÁVACÍCH PAMĚTÍ	hlq.ALTER.BUFFPOOL	ALTER	Bez kontroly	-
ALTER CFSTRUCT	hlq.ALTER.CFSTRUCT	ALTER	Bez kontroly	-
POZMĚNIT KANÁL	hlq.ALTER.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
ALTER NAMELIST	hlq.ALTER.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
ALTER PROCESS	hlq.ALTER.PROCESS	ALTER	hlq.PROCESS.process	ALTER
ALTER PSID	hlq.ALTER.PSID	ALTER	Bez kontroly	-
ALTER QALIAS	hlq.ALTER.QALIAS	ALTER	hlq.QUEUE.queue	ALTER
ALTER QLOCAL“5” na stránce 226	hlq.ALTER.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
ALTER QMGR	hlq.ALTER.QMGR	ALTER	Bez kontroly	-
ALTER QMODEL“5” na stránce 226	hlq.ALTER.QMODEL	ALTER	hlq.QUEUE.queue	ALTER
ZMĚNA QREMOTE	hlq.ALTER.QREMOTE	ALTER	hlq.QUEUE.queue	ALTER

Tabulka 49. Příkazy MQSC, profily a jejich úrovně přístupu (pokračování)

Příkaz	Profil příkazu pro MQCMDS	Úroveň přístupu pro MQCMDS	Profil prostředku příkazu pro MQADMIN nebo MXADMIN	Úroveň přístupu pro MQADMIN nebo MXADMIN
ZMĚNA ZABEZPEČENÍ	hlq.ALTER.SECURITY	ALTER	Bez kontroly	-
ALTER SMDS	hlq.ALTER.SMDS	ALTER	Bez kontroly	-
ALTER STGCLASS	hlq.ALTER.STGCLASS	ALTER	Bez kontroly	-
ALTER SUB	hlq.ALTER.SUB	ALTER	Bez kontroly	-
ALTER TOPIC	hlq.ALTER.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
ALTER TRACE	hlq.ALTER.TRACE	ALTER	Bez kontroly	-
PROTOKOL ARCHIVACE	hlq.ARCHIVE.LOG	CONTROL	Bez kontroly	-
ZÁLOŽNÍ CFSTRUCT	hlq.BACKUP.CFSTRUCT	CONTROL	Bez kontroly	-
VYMAZAT QLOCAL	hlq.CLEAR.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
VYMAZAT TOPICSTR “3” na stránce 226	hlq.CLEAR.TOPICSTR	ALTER	hlq.TOPIC.topic	ALTER
PŘEDEFINOVÁNO AUTHINFO	hlq.DEFINE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
DEFINICE FONDU VYROVNÁVACÍCH PAMĚTÍ	hlq.DEFINE.BUFFPOOL	ALTER	Bez kontroly	-
DEFINE CFSTRUCT	hlq.DEFINE.CFSTRUCT	ALTER	Bez kontroly	-
Definovat kanál	hlq.DEFINE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
DEFINOVANÝ PROTOKOL	hlq.DEFINE.LOG	ALTER	Bez kontroly	-
PŘEDEFINOVÁNO MAXSMSGS	hlq.DEFINE.MAXSMSGS	ALTER	Bez kontroly	-
DEFINE NAMELIST	hlq.DEFINE.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
DEFINOVAT PROCES	hlq.DEFINE.PROCESS	ALTER	hlq.PROCESS.process	ALTER
PŘEDEFINOVÁNO PSID	hlq.DEFINE.PSID	ALTER	Bez kontroly	-
DEFINICE QALIAS	hlq.DEFINE.QALIAS	ALTER	hlq.QUEUE.queue	ALTER
DEFINICE QLOCAL“5” na stránce 226	hlq.DEFINE.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
DEFINICE MODELU QMODEL“5” na stránce 226	hlq.DEFINE.QMODEL	ALTER	hlq.QUEUE.queue	ALTER
DEFINICE QREMOTE	hlq.DEFINE.QREMOTE	ALTER	hlq.QUEUE.queue	ALTER

Tabulka 49. Příkazy MQSC, profily a jejich úrovně přístupu (pokračování)

Příkaz	Profil příkazu pro MQCMDS	Úroveň přístupu pro MQCMDS	Profil prostředku příkazu pro MQADMIN nebo MXADMIN	Úroveň přístupu pro MQADMIN nebo MXADMIN
DEFINOVAT TŘÍDU STGCLASS	hlq.DEFINE.STGCLASS	ALTER	Bez kontroly	-
DEFINE SUB	hlq.DEFINE.SUB	ALTER	Bez kontroly	-
DEFINOVAT TÉMA	hlq.DEFINE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
DELETE AUTHINFO (ODSTRANĚNÍ)	hlq.DELETE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
ODSTRANIT FOND VYROVNÁVACÍCH PAMĚTÍ	hlq.DELETE.BUFFPOOL	ALTER	Bez kontroly	-
DELETE CFSTRUCT (ODSTRANĚNÍ)	hlq.DELETE.CFSTRUCT	ALTER	Bez kontroly	-
Odstranit kanál	hlq.DELETE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
Odstranit seznam názvů	hlq.DELETE.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
Odstranit proces	hlq.DELETE.PROCESS	ALTER	hlq.PROCESS.process	ALTER
Odstranit PSID	hlq.DELETE.PSID	ALTER	Bez kontroly	-
ODSTRANIT QALIAS	hlq.DELETE.QALIAS	ALTER	hlq.QUEUE.queue	ALTER
ODSTRANIT QLOCAL	hlq.DELETE.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
DELETE QMODEL (ODSTRANĚNÍ)	hlq.DELETE.QMODEL	ALTER	hlq.QUEUE.queue	ALTER
ODSTRANIT QREMOTE	hlq.DELETE.QREMOTE	ALTER	hlq.QUEUE.queue	ALTER
ODSTRANIT STGCLASS	hlq.DELETE.STGCLASS	ALTER	Bez kontroly	-
ODSTRANIT SUB	hlq.DELETE.SUB	ALTER	Bez kontroly	-
Odstranit téma	hlq.DELETE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
ZOBRAZIT ARCHIV “1” na stránce 226	hlq.DISPLAY.ARCHIVE	READ (čtení)	Bez kontroly	-
ZOBRAZENÍ AUTHINFO	hlq.DISPLAY.AUTHINFO	READ (čtení)	Bez kontroly	-
ZOBRAZENÍ STAVU CFXX_ENCODE_CASE_CAPS_LOCK_OFF	hlq.DISPLAY.CFSTATUS	READ (čtení)	Bez kontroly	-
ZOBRAZENÍ STRUKTURY CFSTRUCT	hlq.DISPLAY.CFSTRUCT	READ (čtení)	Bez kontroly	-

Tabulka 49. Příkazy MQSC, profily a jejich úrovně přístupu (pokračování)

Příkaz	Profil příkazu pro MQCMDS	Úroveň přístupu pro MQCMDS	Profil prostředku příkazu pro MQADMIN nebo MXADMIN	Úroveň přístupu pro MQADMIN nebo MXADMIN
KANÁL ZOBRAZENÍ	hlq.DISPLAY.CHANNEL	READ (čtení)	Bez kontroly	-
ZOBRAZIT CHINIT	hlq.DISPLAY.CHINIT	READ (čtení)	Bez kontroly	-
ZOBRAZIT CHLAUTH	hlq.DISPLAY.CHLAUTH	READ (čtení)	Bez kontroly	-
ZOBRAZENÍ STAVU CHSTATUS	hlq.DISPLAY.CHSTATUS	READ (čtení)	Bez kontroly	-
ZOBRAZENÍ SOUBORU CLUSQMGR	hlq.DISPLAY.CLUSQMGR	READ (čtení)	Bez kontroly	-
ZOBRAZENÍ CMDSERV	hlq.DISPLAY.CMDSERV	READ (čtení)	Bez kontroly	-
ZOBRAZENÍ PŘIPOJENÍ “1” na stránce 226	hlq.DISPLAY.CONN	READ (čtení)	Bez kontroly	-
Zobrazit skupinu	hlq.DISPLAY.GROUP	READ (čtení)	Bez kontroly	-
ZOBRAZENÍ PROTOKOLU “1” na stránce 226	hlq.DISPLAY.LOG	READ (čtení)	Bez kontroly	-
ZOBRAZENÍ MAXSMSGS	hlq.DISPLAY.MAXSMSGS	READ (čtení)	Bez kontroly	-
ZOBRAZIT SEZNAM NAMELIST	hlq.DISPLAY.NAMELIST	READ (čtení)	Bez kontroly	-
PROCES ZOBRAZENÍ	hlq.DISPLAY.PROCESS	READ (čtení)	Bez kontroly	-
ZOBRAZIT PUBSUB	hlq.DISPLAY.PUBSUB	READ (čtení)	Bez kontroly	-
ZOBRAZENÍ ALIASU QALIAS	hlq.DISPLAY.QALIAS	READ (čtení)	Bez kontroly	-
ZOBRAZENÍ KLASTRU QCLUSTER	hlq.DISPLAY.QCLUSTER	READ (čtení)	Bez kontroly	-
ZOBRAZENÍ QLOCAL	hlq.DISPLAY.QLOCAL	READ (čtení)	Bez kontroly	-
ZOBRAZENÍ SPRÁVCE FRONT	hlq.DISPLAY.QMGR	READ (čtení)	Bez kontroly	-
ZOBRAZENÍ MODELU QMODEL	hlq.DISPLAY.QMODEL	READ (čtení)	Bez kontroly	-

Tabulka 49. Příkazy MQSC, profily a jejich úrovně přístupu (pokračování)

Příkaz	Profil příkazu pro MQCMDS	Úroveň přístupu pro MQCMDS	Profil prostředku příkazu pro MQADMIN nebo MXADMIN	Úroveň přístupu pro MQADMIN nebo MXADMIN
ZOBRAZENÍ QREMOTE	hlq.DISPLAY.QREMOTE	READ (čtení)	Bez kontroly	-
ZOBRAZENÍ STAVU QSTATUS	hlq.DISPLAY.QSTATUS	READ (čtení)	Bez kontroly	-
FRONTA ZOBRAZENÍ	hlq.DISPLAY.QUEUE	READ (čtení)	Bez kontroly	-
ZOBRAZENÍ STAVU SBSTATUS	hlq.DISPLAY.SBSTATUS	READ (čtení)	Bez kontroly	-
Zobrazit sadu SMDS	hlq.DISPLAY.SMDS	READ (čtení)	Bez kontroly	-
ZOBRAZENÍ SMDSCONN	hlq.DISPLAY.SMDSCONN	READ (čtení)	Bez kontroly	-
DÍLČÍ ZOBRAZENÍ	hlq.DISPLAY.SUB	READ (čtení)	Bez kontroly	-
ZOBRAZENÍ ZABEZPEČENÍ	hlq.DISPLAY.SECURITY	READ (čtení)	Bez kontroly	-
ZOBRAZENÍ STGCLASS	hlq.DISPLAY.STGCLASS	READ (čtení)	Bez kontroly	-
ZOBRAZENÍ SYSTÉMU “1” na stránce 226	hlq.DISPLAY.SYSTEM	READ (čtení)	Bez kontroly	-
ZOBRAZENÍ VLÁKNA	hlq.DISPLAY.THREAD	READ (čtení)	Bez kontroly	-
ZOBRAZIT TPSTATUS	hlq.DISPLAY.TPSTATUS	READ (čtení)	Bez kontroly	-
ZOBRAZIT TÉMA	hlq.DISPLAY.TOPIC	READ (čtení)	Bez kontroly	-
ZOBRAZIT TPSTATUS	hlq.DISPLAY.TPSTATUS	READ (čtení)	Bez kontroly	-
ZOBRAZENÍ TRASOVÁNÍ	hlq.DISPLAY.TRACE	READ (čtení)	Bez kontroly	-
Zobrazení využití“1” na stránce 226	hlq.DISPLAY.USAGE	READ (čtení)	Bez kontroly	-
PŘESUNOUT QLOCAL	hlq.MOVE.QLOCAL	ALTER	hlq.QUEUE.from-queue hlq.QUEUE.to-queue	ALTER
Odeslat signál Ping pro kanál	hlq.PING.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Obnovit BSDS	hlq.RECOVER.BSDS	CONTROL	Bez kontroly	-

Tabulka 49. Příkazy MQSC, profily a jejich úrovně přístupu (pokračování)

Příkaz	Profil příkazu pro MQCMDS	Úroveň přístupu pro MQCMDS	Profil prostředku příkazu pro MQADMIN nebo MXADMIN	Úroveň přístupu pro MQADMIN nebo MXADMIN
ZOTAVENÍ CFSTRUCT	hlq.RECOVER.CFSTRUCT	CONTROL	Bez kontroly	-
Aktualizovat klastr	hlq.REFRESH.CLUSTER	ALTER	Bez kontroly	-
AKTUALIZOVAT SPRÁVCE FRONT	hlq.REFRESH.QMGR	ALTER	Bez kontroly	-
REFRESH SECURITY	hlq.REFRESH.SECURITY	ALTER	Bez kontroly	-
RESET CFSTRUCT	hlq.RESET.CFSTRUCT	CONTROL	Bez kontroly	-
Resetovat kanál	hlq.RESET.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Reset klastru	hlq.RESET.CLUSTER	CONTROL	Bez kontroly	-
RESET QMGR	hlq.RESET.QMGR	CONTROL	Bez kontroly	-
RESETOVAT QSTATS	hlq.RESET.QSTATS	CONTROL	hlq.QUEUE.queue	CONTROL
Resetovat SMDS	hlq.RESET.SMDS	CONTROL	Bez kontroly	-
Obnovit položku Tpipe	hlq.RESET.TPIPE	CONTROL	Bez kontroly	-
Vyřešit kanál	hlq.RESOLVE.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Vyřešit nejisté položky	hlq.RESOLVE.INDOUBT	CONTROL	Bez kontroly	-
OBNOVTE SPRÁVCE FRONT	hlq.RESUME.QMGR	CONTROL	Bez kontroly	-
RVERIFY ZABEZPEČENÍ	hlq.RVERIFY.SECURITY	ALTER	Bez kontroly	-
Nastavit archiv	hlq.SET.ARCHIVE	CONTROL	Bez kontroly	-
NASTAVIT CHLAUTH	hlq.SET.CHLAUTH	CONTROL	Bez kontroly	-
Nastavit protokol	hlq.SET.LOG	CONTROL	Bez kontroly	-
Nastavit systém	hlq.SET.SYSTEM	CONTROL	Bez kontroly	-
Spustit kanál	hlq.START.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
START CHINIT “4” na stránce 226	hlq.START.CHINIT	CONTROL	Bez kontroly	-
START CMDSERV	hlq.START.CMDSERV	CONTROL	Bez kontroly	-
Spustit listener	hlq.START.LISTENER	CONTROL	Bez kontroly	-
Začátek QMGR	Není“2” na stránce 226	-	-	-
Spuštění SMDSCONN	hlq.START.SMDSCONN	CONTROL	Bez kontroly	-
Spustit trasování	hlq.START.TRACE	CONTROL	Bez kontroly	-
Ukončit kanál	hlq.STOP.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
ZASTAVTE CHINIT	hlq.STOP.CHINIT	CONTROL	Bez kontroly	-

Tabulka 49. Příkazy MQSC, profily a jejich úrovně přístupu (pokračování)				
Příkaz	**Profil příkazu pro MQCMDS**	**Úroveň přístupu pro MQCMDS**	**Profil prostředku příkazu pro MQADMIN nebo MXADMIN**	**Úroveň přístupu pro MQADMIN nebo MXADMIN**
STOP CMDSERV	hlq.STOP.CMDSERV	CONTROL	Bez kontroly	-
Ukončit listener	hlq.STOP.LISTENER	CONTROL	Bez kontroly	-
STOP QMGR	hlq.STOP.QMGR	CONTROL	Bez kontroly	-
STOP SMDSCONN	hlq.STOP.SMDSCONN	CONTROL	Bez kontroly	-
Zastavit trasování	hlq.STOP.TRACE	CONTROL	Bez kontroly	-
SUSPEND QMgr	hlq.SUSPEND.QMGR	CONTROL	Bez kontroly	-

Notes:

1. Tyto příkazy mohou být vydány interně správcem front; v těchto případech není kontrolováno žádné oprávnění.
2. Produkt IBM MQ nekontroluje oprávnění uživatele, který zadal příkaz START QMGR. K řízení přístupu k příkazu START xxxxMSTR , který je vydán jako výsledek příkazu START QMGR, však můžete použít produkt RACFnebo alternativní prostředky zabezpečení.

   To se provádí řízením přístupu k profilu MVS.START.STC.xxxxMSTR ve třídě příkazů operátora RACF (OPERCMDS). Podrobnosti o této proceduře viz Udělování uživatelského přístupu ke třídě RACF OPERCMDS v tématu *z/OS MVS Plánování: Operace*. Pokud použijete tuto techniku a neautorizovaný uživatel se pokusí spustit správce front, bude ukončen s kódem příčiny 00F30216.
3. Prostředek **hlq.TOPIC.topic** odkazuje na objekt Topic odvozený od objektu TOPICSTR. Další podrobnosti viz "Zabezpečení publikování/odběru" na stránce 501
4. V souboru IBM MQ for z/OSse jedná o název prostředku MVS.START.STC.CSQ1CHIN má připojen další kvalifikátor JOBNAME. To může způsobit problémy při spouštění inicializátoru kanálu.

   Chcete-li vyřešit problém, nahraďte parametr MVS.START.STC. *ssid* CHIN s profilem pro prostředek s názvem MVS.START.STC. *ssid* CHIN **.*** nebo MVS.START.STC. *ssid* CHIN. *ssid* CHIN, kde *ssid* je ID subsystému pro správce front. To vyžaduje oprávnění RACF UPDATE. Další podrobnosti viz MVS Příkazy, RACF přístupové autority a názvy prostředků v části *z/OS MVS Plánování: Operace*.

   Příkaz START pro *ssid* MSTR nezahrnuje parametr JOBNAME=. V zájmu konzistence můžete aktualizovat profil pro MVS.START.STC.ssidMSTR na MVS.START.STC.ssidMSTR. *.
5. V 9.3.0 Nastavení atributu fronty STREAMQ na neprázdnou hodnotu také vyžaduje úroveň přístupu ALTER pro MQADMIN nebo MXADMIN pro `hlq.ALTER.streamQ`.

Tabulka 50. Příkazy PCF, profily a jejich úrovně přístupu				
Příkaz	**Profil příkazu pro MQCMDS**	**Úroveň přístupu pro MQCMDS**	**Profil prostředku příkazu pro MQADMIN nebo MXADMIN**	**Úroveň přístupu pro MQADMIN nebo MXADMIN**
Zálohovat strukturu CF	hlq.BACKUP.CFSTRUCT	CONTROL	Bez kontroly	-
Změnit objekt ověřovacích informací	hlq.ALTER.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
Změnit strukturu CF	hlq.ALTER.CFSTRUCT	ALTER	Bez kontroly	-

Tabulka 50. Příkazy PCF, profily a jejich úrovně přístupu (pokračování)

Příkaz	Profil příkazu pro MQCMDS	Úroveň přístupu pro MQCMDS	Profil prostředku příkazu pro MQADMIN nebo MXADMIN	Úroveň přístupu pro MQADMIN nebo MXADMIN
Změnit kanál	hlq.ALTER.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
Změnit seznam názvů	hlq.ALTER.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
Změnit proces	hlq.ALTER.PROCESS	ALTER	hlq.PROCESS.process	ALTER
Změnit frontu“2” na stránce 230	hlq.ALTER.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
Změnit správce front	hlq.ALTER.QMGR	ALTER	Bez kontroly	-
Změna zabezpečení	hlq.ALTER.SECURITY	ALTER	Bez kontroly	-
Změnit SMDS	hlq.ALTER.SMDS	ALTER	Bez kontroly	-
Změnit úložnou třídu	hlq.ALTER.STGCLASS	ALTER	Bez kontroly	-
Změnit odběr	hlq.ALTER.SUB	ALTER	Bez kontroly	-
Změnit téma	hlq.ALTER.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
Vymazat frontu	hlq.CLEAR.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
Vymazat řetězec tématu“1” na stránce 230	hlq.CLEAR.TOPICSTR	ALTER	hlq.TOPIC.topic	ALTER
Kopírovat objekt ověřovacích informací	hlq.DEFINE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
Kopírovat strukturu CF	hlq.DEFINE.CFSTRUCT	ALTER	Bez kontroly	-
Kopírovat kanál	hlq.DEFINE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
Kopírovat seznam názvů	hlq.DEFINE.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
Kopírovat proces	hlq.DEFINE.PROCESS	ALTER	hlq.PROCESS.process	ALTER
Kopírovat frontu	hlq.DEFINE.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
Kopírovat odběr	hlq.DEFINE.SUB	ALTER	Bez kontroly	-
Kopírovat úložnou třídu	hlq.DEFINE.STGCLASS	ALTER	Bez kontroly	-
Kopírovat téma	hlq.DEFINE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
Vytvořit objekt ověřovacích informací	hlq.DEFINE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
Vytvořit strukturu CF	hlq.DEFINE.CFSTRUCT	ALTER	Bez kontroly	-
Vytvořit kanál	hlq.DEFINE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
Vytvořit seznam názvů	hlq.DEFINE.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
Vytvořit proces	hlq.DEFINE.PROCESS	ALTER	hlq.PROCESS.process	ALTER
Vytvořit frontu“2” na stránce 230	hlq.DEFINE.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
Vytvořit úložnou třídu	hlq.DEFINE.STGCLASS	ALTER	Bez kontroly	-
Vytvořit odběr	hlq.DEFINE.SUB	ALTER	Bez kontroly	-
Vytvořit téma	hlq.DEFINE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER

Tabulka 50. Příkazy PCF, profily a jejich úrovně přístupu (pokračování)

Příkaz	Profil příkazu pro MQCMDS	Úroveň přístupu pro MQCMDS	Profil prostředku příkazu pro MQADMIN nebo MXADMIN	Úroveň přístupu pro MQADMIN nebo MXADMIN
Odstranit objekt ověřovacích informací	hlq.DELETE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
Odstranit strukturu CF	hlq.DELETE.CFSTRUCT	ALTER	Bez kontroly	-
Odstranit kanál	hlq.DELETE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
Odstranit seznam názvů	hlq.DELETE.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
Odstranit proces	hlq.DELETE.PROCESS	ALTER	hlq.PROCESS.process	ALTER
Odstranit frontu	hlq.DELETE.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
Odstranit úložnou třídu	hlq.DELETE.STGCLASS	ALTER	Bez kontroly	-
Odstranit odběr	hlq.DELETE.SUB	ALTER	Bez kontroly	-
Odstranit téma	hlq.DELETE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
Zjistit archiv	hlq.DISPLAY.ARCHIVE	READ (čtení)	Bez kontroly	-
Dotázat se na objekt ověřovacích informací	hlq.DISPLAY.AUTHINFO	READ (čtení)	Bez kontroly	-
Zjistit názvy objektů ověřovacích informací	hlq.DISPLAY.AUTHINFO	READ (čtení)	Bez kontroly	-
Zjistit strukturu CF	hlq.DISPLAY.CFSTRUCT	READ (čtení)	Bez kontroly	-
Zjistit názvy struktury CF	hlq.DISPLAY.CFSTRUCT	READ (čtení)	Bez kontroly	-
Zjistit stav struktury CF	hlq.DISPLAY.CFSTATUS	READ (čtení)	Bez kontroly	-
Zjistit kanál	hlq.DISPLAY.CHANNEL	READ (čtení)	Bez kontroly	-
Zjistit záznam ověření kanálu	hlq.DISPLAY.CHLAUTH	READ (čtení)	Bez kontroly	-
Iniciátor dotazovacího kanálu	hlq.DISPLAY.CHINIT	READ (čtení)	Bez kontroly	-
Zjistit názvy kanálů	hlq.DISPLAY.CHANNEL	READ (čtení)	Bez kontroly	-
Zjistit stav kanálu	hlq.DISPLAY.CHSTATUS	READ (čtení)	Bez kontroly	-
Zjistit správce front klastru	hlq.DISPLAY.CLUSQMGR	READ (čtení)	Bez kontroly	-
Zjistit připojení	hlq.DISPLAY.CONNPCF	READ (čtení)	Bez kontroly	-
Zjistit skupinu	hlq.DISPLAY.GROUP	READ (čtení)	Bez kontroly	-
Zjistit protokol	hlq.DISPLAY.LOG	READ (čtení)	Bez kontroly	-
Zjistit seznam názvů	hlq.DISPLAY.NAMELIST	READ (čtení)	Bez kontroly	-
Zjistit názvy seznamů názvů	hlq.DISPLAY.NAMELIST	READ (čtení)	Bez kontroly	-
Zjistit proces	hlq.DISPLAY.PROCESS	READ (čtení)	Bez kontroly	-
Zjistit názvy procesů	hlq.DISPLAY.PROCESS	READ (čtení)	Bez kontroly	-
Zjistit stav publikování/ odběru	hlq.DISPLAY.PUBSUB	READ (čtení)	Bez kontroly	-

Tabulka 50. Příkazy PCF, profily a jejich úrovně přístupu (pokračování)

Příkaz	Profil příkazu pro MQCMDS	Úroveň přístupu pro MQCMDS	Profil prostředku příkazu pro MQADMIN nebo MXADMIN	Úroveň přístupu pro MQADMIN nebo MXADMIN
Zjistit frontu	hlq.DISPLAY.QUEUE	READ (čtení)	Bez kontroly	-
Zjistit správce front	hlq.DISPLAY.QMGR	READ (čtení)	Bez kontroly	-
Zjistit názvy front	hlq.DISPLAY.QUEUE	READ (čtení)	Bez kontroly	-
Zjistit stav fronty	hlq.DISPLAY.QSTATUS	READ (čtení)	Bez kontroly	-
Zjistit zabezpečení	hlq.DISPLAY.SECURITY	READ (čtení)	Bez kontroly	-
Zjistit SMDS	hlq.DISPLAY.SMDS	READ (čtení)	Bez kontroly	-
Zjistit SMDSCONN	hlq.DISPLAY.SMDSCONN	READ (čtení)	Bez kontroly	-
Zjistit úložnou třídu	hlq.DISPLAY.STGCLASS	READ (čtení)	Bez kontroly	-
Zjistit názvy úložné třídy	hlq.DISPLAY.STGCLASS	READ (čtení)	Bez kontroly	-
Zjistit odběr	hlq.INQUIRE.SUB	READ (čtení)	Bez kontroly	-
Zjistit stav odběru	hlq.INQUIRE.SBSTATUS	READ (čtení)	Bez kontroly	-
Zjistit systém	hlq.DISPLAY.SYSTEM	READ (čtení)	Bez kontroly	-
Zjistit téma	hlq.DISPLAY.TOPIC	READ (čtení)	Bez kontroly	-
Zjistit názvy témat	hlq.DISPLAY.TOPIC	READ (čtení)	Bez kontroly	-
Zjistit stav tématu	hlq.DISPLAY.TPSTATUS	READ (čtení)	Bez kontroly	-
Zjistit použití	hlq.DISPLAY.USAGE	READ (čtení)	Bez kontroly	-
Přesunout frontu	hlq.MOVE.QLOCAL	ALTER	hlq.QUEUE.from-queue hlq.QUEUE.to-queue	ALTER
Odeslat signál Ping pro kanál	hlq.PING.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Obnovit strukturu CF	hlq.RECOVER.CFSTRUCT	CONTROL	Bez kontroly	-
Aktualizovat klastr	hlq.REFRESH.CLUSTER	ALTER	Bez kontroly	-
Aktualizovat správce front	hlq.REFRESH.QMGR	ALTER	Bez kontroly	-
Aktualizovat zabezpečení	hlq.REFRESH.SECURITY	ALTER	Bez kontroly	-
Resetovat strukturu CF	hlq.RESET.CFSTRUCT	CONTROL	Bez kontroly	-
Resetovat kanál	hlq.RESET.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Reset klastru	hlq.RESET.CLUSTER	CONTROL	Bez kontroly	-
Obnovit správce front	hlq.RESET.QMGR	CONTROL	Bez kontroly	-
Obnovit statistiku front	hlq.RESET.QSTATS	CONTROL	hlq.QUEUE.queue	CONTROL
Resetovat SMDS	hlq.RESET.SMDS	CONTROL	Bez kontroly	-
Vyřešit kanál	hlq.RESOLVE.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Obnovit správce front	hlq.RESUME.QMGR	CONTROL	Bez kontroly	-
Obnovit klastr správců front	hlq.RESUME.QMGR	CONTROL	Bez kontroly	-

Tabulka 50. Příkazy PCF, profily a jejich úrovně přístupu (pokračování)				
Příkaz	**Profil příkazu pro MQCMDS**	**Úroveň přístupu pro MQCMDS**	**Profil prostředku příkazu pro MQADMIN nebo MXADMIN**	**Úroveň přístupu pro MQADMIN nebo MXADMIN**
Znovu ověřit zabezpečení	hlq.RVERIFY.SECURITY	ALTER	Bez kontroly	-
Nastavit archiv	hlq.SET.ARCHIVE	CONTROL	Bez kontroly	-
Nastavit záznam ověření kanálu	hlq.SET.CHLAUTH	CONTROL	Bez kontroly	-
Nastavit protokol	hlq.SET.LOG	CONTROL	Bez kontroly	-
Nastavit systém	hlq.SET.SYSTEM	CONTROL	Bez kontroly	-
Spustit kanál	hlq.START.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Spustit inicializátor kanálu	hlq.START.CHINIT	CONTROL	Bez kontroly	-
Spustit modul listener kanálu	hlq.START.LISTENER	CONTROL	Bez kontroly	-
Spustit připojení SMDS	hlq.START.SMDSCONN	CONTROL	Bez kontroly	-
Ukončit kanál	hlq.STOP.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Zastavit inicializátor kanálu	hlq.STOP.CHINIT	CONTROL	Bez kontroly	-
Zastavit modul listener kanálu	hlq.STOP.LISTENER	CONTROL	Bez kontroly	-
Zastavit připojení SMDS	hlq.STOP.SMDSCONN	CONTROL	Bez kontroly	-
Pozastavit správce front	hlq.SUSPEND.QMGR	CONTROL	Bez kontroly	-
Pozastavit klastr správců front	hlq.SUSPEND.QMGR	CONTROL	Bez kontroly	-

Notes:

1. Prostředek **`hlq.TOPIC.topic`** odkazuje na objekt Topic odvozený od objektu TOPICSTR. Další podrobnosti viz “Zabezpečení publikování/odběru” na stránce 501
2. V 9.3.0 Nastavení atributu fronty STREAMQ na neprázdnou hodnotu také vyžaduje úroveň přístupu ALTER pro MQADMIN nebo MXADMIN pro `hlq.ALTER.streamQ`.

Podrobné informace o vyžadovaných profilech PCF systému IBM MQ při použití konzoly IBM MQ Consolenaleznete v části “IBM MQ Console -povinné profily zabezpečení příkazu” na stránce 230 .

z/OS *IBM MQ Console -povinné profily zabezpečení příkazu*

Operace provedené v souboru IBM MQ Console uživatelem v roli `MQWebAdmin`nebo `MQWebAdminRO`se provádějí v kontextu zabezpečení ID uživatele spuštěné úlohy serveru mqweb. Chcete-li použít IBM MQ Console, ID uživatele spuštěné úlohy serveru mqweb potřebuje autorizaci k zadání určitých příkazů PCF.

V tabulce Tabulka 51 na stránce 231 jsou pro každý příkaz IBM MQ PCF uvedeny požadované profily zabezpečení příkazu a odpovídající úroveň přístupu pro každý profil ve třídě MQCMDS potřebné pro IBM MQ Console.

Tabulka 51. IBM MQ Console příkazy PCF, profily a jejich úrovně přístupu

Příkaz	Profil příkazu pro MQCMDS	Úroveň přístupu pro MQCMDS	Profil prostředku příkazu pro MQADMIN nebo MXADMIN	Úroveň přístupu pro MQADMIN nebo MXADMIN
Změnit objekt ověřovacích informací	hlq.ALTER.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
Změnit kanál	hlq.ALTER.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
Změnit frontu	hlq.ALTER.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
Změnit správce front	hlq.ALTER.QMGR	ALTER	Bez kontroly	-
Změnit téma	hlq.ALTER.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
Vymazat frontu	hlq.CLEAR.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
Vytvořit objekt ověřovacích informací	hlq.DEFINE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
Vytvořit kanál	hlq.DEFINE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
Vytvořit frontu	hlq.DEFINE.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
Vytvořit odběr	hlq.DEFINE.SUB	ALTER	Bez kontroly	-
Vytvořit téma	hlq.DEFINE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
Odstranit objekt ověřovacích informací	hlq.DELETE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
Odstranit kanál	hlq.DELETE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
Odstranit frontu	hlq.DELETE.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
Odstranit odběr	hlq.DELETE.SUB	ALTER	Bez kontroly	-
Odstranit téma	hlq.DELETE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
Dotázat se na objekt ověřovacích informací	hlq.DISPLAY.AUTHINFO	READ (čtení)	Bez kontroly	-
Zjistit názvy objektů ověřovacích informací	hlq.DISPLAY.AUTHINFO	READ (čtení)	Bez kontroly	-
Zjistit kanál	hlq.DISPLAY.CHANNEL	READ (čtení)	Bez kontroly	-
Zjistit záznam ověření kanálu	hlq.DISPLAY.CHLAUTH	READ (čtení)	Bez kontroly	-
Iniciátor dotazovacího kanálu	hlq.DISPLAY.CHINIT	READ (čtení)	Bez kontroly	-
Zjistit názvy kanálů	hlq.DISPLAY.CHANNEL	READ (čtení)	Bez kontroly	-
Zjistit stav kanálu	hlq.DISPLAY.CHSTATUS	READ (čtení)	Bez kontroly	-
Zjistit frontu	hlq.DISPLAY.QUEUE	READ (čtení)	Bez kontroly	-
Zjistit správce front	hlq.DISPLAY.QMGR	READ (čtení)	Bez kontroly	-
Zjistit názvy front	hlq.DISPLAY.QUEUE	READ (čtení)	Bez kontroly	-
Zjistit stav fronty	hlq.DISPLAY.QSTATUS	READ (čtení)	Bez kontroly	-
Zjistit odběr	hlq.INQUIRE.SUB	READ (čtení)	Bez kontroly	-
Zjistit stav odběru	hlq.INQUIRE.SBSTATUS	READ (čtení)	Bez kontroly	-
Zjistit téma	hlq.DISPLAY.TOPIC	READ (čtení)	Bez kontroly	-

Tabulka 51. IBM MQ Console příkazy PCF, profily a jejich úrovně přístupu (pokračování)				
Příkaz	**Profil příkazu pro MQCMDS**	**Úroveň přístupu pro MQCMDS**	**Profil prostředku příkazu pro MQADMIN nebo MXADMIN**	**Úroveň přístupu pro MQADMIN nebo MXADMIN**
Zjistit názvy témat	hlq.DISPLAY.TOPIC	READ (čtení)	Bez kontroly	-
Zjistit stav tématu	hlq.DISPLAY.TPSTATUS	READ (čtení)	Bez kontroly	-
Odeslat signál Ping pro kanál	hlq.PING.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Aktualizovat klastr	hlq.REFRESH.CLUSTER	ALTER	Bez kontroly	-
Aktualizovat zabezpečení	hlq.REFRESH.SECURITY	ALTER	Bez kontroly	-
Resetovat kanál	hlq.RESET.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Vyřešit kanál	hlq.RESOLVE.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Nastavit záznam ověření kanálu	hlq.SET.CHLAUTH	CONTROL	Bez kontroly	-
Spustit kanál	hlq.START.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Ukončit kanál	hlq.STOP.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL

z/OS *Profily pro zabezpečení prostředků příkazu*

Pokud jste nedefinovali profil přepínače zabezpečení prostředků příkazu, protože chcete kontrolovat zabezpečení prostředků přidružených k příkazům, musíte přidat profily prostředků pro každý prostředek do příslušné třídy. Stejné profily zabezpečení řídí příkazy MQSC i PCF.

Pokud jste nedefinovali profil přepínače zabezpečení prostředků příkazu `hlq.NO.CMD.RESC.CHECKS`, protože chcete kontrolovat zabezpečení prostředků přidružených k příkazům, musíte:

- Přidejte profil prostředku do třídy **MQADMIN** , pokud používáte profily s velkými písmeny, pro každý prostředek.
- Přidejte profil prostředku do třídy **MXADMIN** , pokud používáte profily se smíšenými velkými a velkými písmeny, pro každý prostředek.

Stejné profily zabezpečení řídí příkazy MQSC i PCF.

Profily pro kontrolu zabezpečení prostředků příkazu jsou ve tvaru:

```
hlq.type.resourcename
```

kde `hlq` může být buď `qmgr-name` (název správce front), nebo `qsg-name` (název skupiny sdílení front).

Profil s předponou názvu správce front řídí přístup k prostředkům přidruženým k příkazům v daném správci front. Profil s předponou názvu skupiny sdílení front řídí přístup k prostředkům přidruženým k příkazům ve všech správcích front v rámci skupiny sdílení front. Tento přístup lze v jednotlivých správcích front potlačit definováním profilu úrovně správce front pro daný prostředek příkazu v daném správci front.

Pokud je váš správce front členem skupiny sdílení front a používáte zabezpečení na úrovni správce front i skupiny sdílení front, produkt IBM MQ nejprve zkontroluje profil s předponou podle názvu správce front. Pokud jej nenajde, vyhledá profil s předponou názvu skupiny sdílení front.

Například název profilu RACF pro kontrolu zabezpečení prostředků příkazů pro modelovou frontu CREDIT.WORTHY v subsystému CSQ1 je:

```
CSQ1.QUEUE.CREDIT.WORTHY
```

Vzhledem k tomu, že profily pro všechny typy prostředků příkazů jsou uloženy ve třídě MQADMIN, je v profilu vyžadována část názvu profilu "type", která rozlišuje mezi prostředky různých typů se stejným názvem. Část "type" názvu profilu může být CHANNEL, QUEUE, TOPIC, PROCESS nebo NAMELIST. Uživatel může být například autorizován k definování souboru hlq.QUEUE.PAYROLL.ONE, ale není autorizován definovat hlq.PROCESS.PAYROLL.ONE

Pokud je typem prostředku fronta a profil je profilem na úrovni skupiny sdílení front, řídí přístup k jedné nebo více lokálním frontám v rámci skupiny sdílení front nebo přístup k jedné sdílené frontě z libovolného správce front ve skupině sdílení front.

Příkazy MQSC, profily a jejich úrovně přístupu zobrazují pro každý příkaz IBM MQ MQSC profily nezbytné pro provedení kontroly zabezpečení příkazů a odpovídající úroveň přístupu pro každý profil ve třídě MQCMDS.

V části Příkazy PCF, profily a jejich úrovně přístupu jsou pro každý příkaz IBM MQ PCF uvedeny profily vyžadované pro provedení kontroly zabezpečení příkazu a odpovídající úroveň přístupu pro každý profil ve třídě MQCMDS.

z/OS *Kontrola zabezpečení prostředků příkazů pro alias fronty a vzdálené fronty*

Alias fronty i vzdálené fronty poskytují nepřímý odkaz na jinou frontu. Další body se použijí, když uvážíte kontrolu zabezpečení pro tyto fronty.

Alias fronty

Definujete-li alias fronty, budou kontroly zabezpečení prostředků příkazů prováděny pouze pro název alias fronty, nikoli pro název cílové fronty, do které se alias převádí.

Fronty aliasů lze interpretovat jako lokální i vzdálené fronty. Pokud nechcete uživatelům povolit přístup k určitým lokálním nebo vzdáleným frontám, musíte provést obě následující akce:

1. Nepovolujte uživatelům přístup k těmto lokálním a vzdáleným frontám.
2. Omezte uživatele, aby mohli definovat aliasy pro tyto fronty. To znamená, že jim zabráníte v tom, aby mohli zadávat příkazy DEFINE QALIAS a ALTER QALIAS.

Vzdálené fronty

Při definování vzdálené fronty jsou kontroly zabezpečení prostředků příkazů prováděny pouze pro název vzdálené fronty. Neprovádějí se žádné kontroly názvů front uvedených v atributech RNAME nebo XMITQ v definici objektu vzdálené fronty.

z/OS Profil zabezpečení RESLEVEL

Můžete definovat speciální profil ve třídě MQADMIN nebo MXADMIN, chcete-li řídit počet ID uživatelů kontrolovaných pro zabezpečení prostředků rozhraní API. Tento profil se nazývá profil RESLEVEL. Způsob, jakým tento profil ovlivňuje zabezpečení prostředků rozhraní API, závisí na způsobu přístupu k produktu IBM MQ.

Když se aplikace pokusí připojit k produktu IBM MQ, produkt IBM MQ zkontroluje přístup, který má ID uživatele přidružené k připojení k profilu ve třídě MQADMIN nebo MXADMIN s názvem:

```
hlq.RESLEVEL
```

Kde `hlq` může být buď `ssid` (ID subsystému), nebo `qsg` (ID skupiny sdílení front).

ID uživatelů přidružená ke každému typu připojení jsou:

- ID uživatele připojující se úlohy pro dávková připojení
- ID uživatele adresního prostoru CICS pro připojení CICS
- ID uživatele adresního prostoru oblasti IMS pro připojení IMS
- ID uživatele adresního prostoru inicializátoru kanálu pro připojení inicializátoru kanálu

Upozornění: RESLEVEL je velmi výkonná volba; může způsobit vynechání všech kontrol zabezpečení prostředků pro konkrétní připojení.

Pokud nemáte definován profil RESLEVEL, musíte být opatrní, aby žádný jiný profil ve třídě MQADMIN neodpovídal hodnotě hlq.RESLEVEL. Máte-li například profil v MQADMIN s názvem hlq. * * a žádný profil hlq.RESLEVEL , pozor na důsledky hlq. * * protože se používá pro kontrolu RESLEVEL.

Definujte profil hlq.RESLEVEL a nastavte UACC na hodnotu NONE, místo abyste měli profil RESLEVEL vůbec. Mějte co nejméně uživatelů nebo skupin v seznamu pro přístup. Podrobnosti o tom, jak auditovat přístup RESLEVEL, viz “Aspekty auditování v systému z/OS” na stránce 258.

Používáte-li pouze zabezpečení na úrovni správce front, produkt IBM MQ provede kontroly RESLEVEL pro profil `qmgr-name.RESLEVEL` . Pokud používáte pouze zabezpečení na úrovni skupiny sdílení front, produkt IBM MQ provede kontroly RESLEVEL pro profil `qsg-name.RESLEVEL` . Pokud používáte kombinaci zabezpečení na úrovni správce front i skupiny sdílení front, produkt IBM MQ nejprve zkontroluje existenci profilu RESLEVEL na úrovni správce front. Pokud jej nenajde, zkontroluje profil RESLEVEL na úrovni skupiny sdílení front.

Pokud nemůže najít profil RESLEVEL, produkt IBM MQ povolí kontrolu úlohy i ID úlohy (nebo alternativního uživatele) pro připojení CICS nebo IMS . V případě dávkového připojení produkt IBM MQ umožňuje kontrolu ID uživatele úlohy (nebo alternativního). Pro inicializátor kanálu produkt IBM MQ umožňuje kontrolu ID uživatele kanálu a ID uživatele MCA (nebo alternativního).

Pokud existuje profil RESLEVEL, úroveň kontroly závisí na prostředí a úrovni přístupu pro profil.

Mějte na paměti, že pokud je váš správce front členem skupiny sdílení front a nedefinujete tento profil na úrovni správce front, může existovat jeden definovaný na úrovni skupiny sdílení front, který bude mít vliv na úroveň kontroly. Chcete-li aktivovat kontrolu dvou ID uživatelů, definujte profil RESLEVEL (s předponou buď s názvem správce front názvu skupiny sdílení front) s UACC (NONE) a ujistěte se, že příslušní uživatelé nemají pro tento profil udělen přístup.

Pokud uvážíte přístup, který má ID uživatele inicializátoru kanálu na hodnotu RESLEVEL, nezapomeňte, že připojení vytvořené inicializátorem kanálu je také připojení používané kanály. Nastavení, které způsobí, že vynechání všech kontrol zabezpečení prostředků pro ID uživatele inicializátoru kanálu účinně vynechá kontroly zabezpečení pro všechny kanály. Je-li přístup ID uživatele inicializátoru kanálu k parametru RESLEVEL jiný než NONE, bude pro přístup kontrolován pouze jeden identifikátor uživatele (pro úroveň přístupu READ nebo UPDATE) nebo žádný identifikátor uživatele (pro úroveň přístupu CONTROL nebo ALTER). Udělíte-li ID uživatele inicializátoru kanálu jinou úroveň přístupu než NONE pro RESLEVEL, ujistěte se, že rozumíte vlivu tohoto nastavení na kontroly zabezpečení prováděné pro kanály.

Použití profilu RESLEVEL znamená, že se neberou normální záznamy auditu zabezpečení. Pokud například umístíte UAUDIT na uživatele, přístup k profilu hlq.RESLEVEL v MQADMIN nebude auditován.

Použijete-li volbu RACF VAROVÁNÍ v profilu hlq.RESLEVEL , nebudou pro profily ve třídě RESLEVEL vytvářeny žádné varovné zprávy RACF .

Kontrola zabezpečení zpráv sestavy, jako např. COD, jsou řízeny profilem RESLEVEL přidruženým k původní aplikaci. Pokud má například ID uživatele dávkové úlohy oprávnění CONTROL nebo ALTER pro profil RESLEVEL, bude veškerá kontrola prostředků prováděná dávkovou úlohou vynechána, včetně kontroly zabezpečení zpráv sestavy.

Změníte-li profil RESLEVEL, uživatelé se musí před provedením změny odpojit a znovu připojit. (To zahrnuje zastavení a restartování inicializátoru kanálu, pokud se změní přístup, který má ID uživatele distribuovaného adresního prostoru fronty k profilu RESLEVEL.)

Chcete-li vypnout auditování RESLEVEL, použijte systémový parametr RESAUDIT.

z/OS *RESLEVEL a dávková připojení*

Standardně, když se k prostředku IBM MQ přistupuje prostřednictvím dávkového připojení a připojení dávkového typu, musí být uživatel autorizován pro přístup k tomuto prostředku pro konkrétní operaci. Kontrolu zabezpečení můžete obejít nastavením odpovídající definice RESLEVEL.

Zda je uživatel kontrolován, či nikoli, je založeno na ID uživatele použitém v době připojení, stejné ID uživatele použité pro kontrolu připojení.

Můžete například nastavit parametr RESLEVEL tak, aby v případě, že uživatel, kterému důvěřujete, přistupuje k určitým prostředkům prostřednictvím dávkového připojení, nebyly provedeny žádné kontroly zabezpečení prostředků rozhraní API. Pokud se však uživatel, kterému důvěřujete, pokusí získat přístup ke stejným prostředkům, budou kontroly zabezpečení prováděny jako obvykle. Měli byste nastavit kontrolu RESLEVEL tak, aby obešla kontroly zabezpečení prostředků rozhraní API pouze v případě, že dostatečně důvěřujete uživateli a programům spuštěným tímto uživatelem.

Následující tabulka zobrazuje kontroly provedené pro dávková připojení.

Tabulka 52. Kontroly provedené na různých úrovních přístupu RACF pro dávková připojení

RACF úroveň přístupu	**Úroveň kontroly**
ŽÁDNÉ	Provedené kontroly prostředků
READ (čtení)	Provedené kontroly prostředků
AKTUALIZOVAT	Provedené kontroly prostředků
CONTROL	Žádný šek.
ALTER	Žádný šek.

z/OS *RESLEVEL a systémové funkce*

Aplikace RESLEVEL na ovládací a ovládací panely a na CSQUTIL.

Operační a řídicí panely a obslužný program CSQUTIL jsou aplikace dávkového typu, které vytvářejí požadavky na příkazový server správce front, a proto se na ně vztahují aspekty popsané v tématu “RESLEVEL a dávková připojení” na stránce 234. Pomocí příkazu RESLEVEL můžete obejít kontrolu zabezpečení pro systém SYSTEM.COMMAND.INPUT a SYSTEM.COMMAND.REPLY.MODEL fronty, které používají, ale ne pro dynamické fronty SYSTEM.CSQXCMD. *, SYSTEM.CSQOREXX.*, a SYSTEM.CSQUTIL. *.

Příkazový server je nedílnou součástí správce front, a proto k němu není přidruženo připojení ani kontrola RESLEVEL. Aby bylo možné zachovat zabezpečení, musí příkazový server potvrdit, že ID uživatele požadující aplikace má oprávnění k otevření fronty používané pro odpovědi. Pro operace a ovládací panely se jedná o SYSTEM.CSQOREXX. *. Pro CSQUTIL je to SYSTEM.CSQUTIL. *. Uživatelé musí být autorizováni k použití těchto front, jak je popsáno v tématu “Zabezpečení systémové fronty” na stránce 206, kromě všech oprávnění RESLEVEL, která jim byla poskytnuta.

Pro ostatní aplikace používající příkazový server je to fronta, kterou pojmenují jako svou frontu pro odpověď. Tyto jiné aplikace mohou oklamat příkazový server při umisťování zpráv do neautorizovaných front předáním (v kontextu zpráv) důvěryhodnějšího ID uživatele, než je jeho vlastní ID příkazového serveru. Chcete-li tomu zabránit, použijte profil CONTEXT k ochraně kontextu identity zpráv umístěných v systému SYSTEM.COMMAND.INPUT.

z/OS *RESLEVEL a CICS připojení*

Standardně, když se provádí kontrola zabezpečení prostředků rozhraní API pro připojení CICS , kontrolují se dvě ID uživatelů. Můžete změnit, která ID uživatelů se kontrolují, nastavením profilu RESLEVEL.

První kontrolované ID uživatele je ID adresního prostoru CICS . Jedná se o ID uživatele na zakázkovém listu úlohy CICS nebo ID uživatele přiřazené ke spuštěné úloze CICS pomocí třídy z/OS STARTED nebo tabulky spuštěných procedur. (Není to CICS DFLTUSER.)

Druhé kontrolované ID uživatele je ID uživatele přidružené k transakci CICS .

Pokud jedno z těchto ID uživatelů nemá přístup k prostředku, požadavek selže s kódem dokončení MQRC_NOT_AUTHORIZED. ID uživatele adresního prostoru CICS i ID uživatele osoby, která spouští transakci CICS , musí mít přístup k prostředku na správné úrovni.

Jak může RESLEVEL ovlivnit provedené kontroly

V závislosti na tom, jak jste nastavili profil RESLEVEL, můžete změnit, která ID uživatelů jsou kontrolována, když je požadován přístup k prostředku. Další informace viz Tabulka 53 na stránce 236.

Kontrolovaná ID uživatelů závisí na ID uživatele použitém v době připojení, tj. na ID uživatele adresního prostoru CICS . Tento ovládací prvek vám umožňuje obejít kontrolu zabezpečení prostředků rozhraní API pro požadavky IBM MQ přicházející z jednoho systému (například testovací systém, TESTCICS), ale implementovat je pro jiný (například produkční systém, PRODCICS).

Poznámka: Pokud nastavíte ID uživatele adresního prostoru CICS pomocí atributu "důvěryhodný" ve třídě STARTED nebo v RACF tabulce spuštěných procedur ICHRIN03, potlačí to všechny kontroly ID uživatele pro adresní prostor CICS vytvořené profilem RESLEVEL pro vašeho správce front (to znamená, že správce front neprovádí kontroly zabezpečení pro adresní prostor CICS). Další informace viz Zabezpečení CICS.

Následující tabulka zobrazuje kontroly provedené pro připojení CICS .

Tabulka 53. Kontroly provedené na různých RACF úrovních přístupu pro připojení CICS

RACF úroveň přístupu	**Úroveň kontroly**
ŽÁDNÉ	IBM MQ kontroluje ID uživatele adresního prostoru CICS a ID uživatele transakce.
READ (čtení)	IBM MQ kontroluje pouze ID uživatele CICS adresního prostoru.
AKTUALIZOVAT	Je-li transakce definována v produktu CICS s volbou RESSEC (YES), produkt IBM MQ zkontroluje ID uživatele adresního prostoru CICS a ID uživatele transakce.
AKTUALIZOVAT	Pokud je transakce definována pro CICS s RESSEC (NO), IBM MQ zkontroluje pouze ID uživatele CICS adresního prostoru.
CONTROL nebo ALTER	Produkt IBM MQ nekontroluje žádná ID uživatelů.

z/OS *RESLEVEL a IMS připojení*

Standardně se při kontrole zabezpečení prostředků rozhraní API pro připojení k systému IMS kontrolují dvě ID uživatelů. Můžete změnit, která ID uživatelů se kontrolují, nastavením profilu RESLEVEL.

Standardně, když je pro připojení IMS provedena kontrola zabezpečení prostředku rozhraní API, jsou zkontrolována dvě ID uživatelů, aby se zjistilo, zda je k prostředku povolen přístup.

První kontrolované ID uživatele je ID adresního prostoru oblasti IMS . Toto je převzato buď z pole USER ze zakázkového listu, nebo z ID uživatele přiřazeného k oblasti ze třídy z/OS STARTED nebo z tabulky spuštěných procedur (SPT).

Druhé kontrolované ID uživatele je přidruženo k práci, která se provádí v závislé oblasti. Určuje se podle typu závislé oblasti, jak ukazuje Způsob určení druhého ID uživatele pro připojení IMS(tm).

Pokud buď první, nebo druhé ID uživatele IMS nemá přístup k prostředku, požadavek selže s kódem dokončení MQRC_NOT_AUTHORIZED.

Nastavení profilů IBM MQ RESLEVEL nemůže změnit ID uživatele, pod kterým jsou naplánovány transakce IMS z programu monitorování spouštěčů IBM-dodaný MQ-IMS CSQQTRMN. Toto ID uživatele je PSBNAME tohoto monitoru spouštěčů, který je standardně CSQQTRMN.

Jak může RESLEVEL ovlivnit provedené kontroly

V závislosti na tom, jak jste nastavili profil RESLEVEL, můžete změnit, která ID uživatelů jsou kontrolována, když je požadován přístup k prostředku. Možné kontroly jsou:

- Zkontrolujte ID uživatele adresního prostoru oblasti IMS a druhé ID uživatele nebo alternativní ID uživatele.
- Zkontrolujte pouze ID uživatele adresního prostoru oblasti IMS .

- Nezaškrtávejte žádná ID uživatelů.

Následující tabulka zobrazuje kontroly provedené pro připojení IMS .

Tabulka 54. Kontroly provedené na různých RACF úrovních přístupu pro připojení IMS	
RACF úroveň přístupu	**Úroveň kontroly**
ŽÁDNÉ	Zkontrolujte ID uživatele adresního prostoru IMS a ID druhého nebo alternativního uživatele IMS .
READ (čtení)	Zkontrolujte ID uživatele adresního prostoru IMS .
AKTUALIZOVAT	Zkontrolujte ID uživatele adresního prostoru IMS .
CONTROL	Žádný šek.
ALTER	Žádný šek.

z/OS *RESLEVEL a připojení inicializátoru kanálu*

Při výchozím nastavení, když iniciátor kanálu provádí kontrolu zabezpečení prostředku rozhraní API, jsou zkontrolována dvě ID uživatelů. Můžete změnit, která ID uživatelů se kontrolují, nastavením profilu RESLEVEL.

Standardně, když iniciátor kanálu provádí kontrolu zabezpečení prostředku rozhraní API, kontrolují se dvě ID uživatelů, aby se zjistilo, zda je k prostředku povolen přístup.

Kontrolovaná ID uživatelů mohou být určena atributem kanálu MCAUSER, která byla přijata ze sítě, adresním prostorem inicializátoru kanálu nebo alternativním ID uživatele pro deskriptor zprávy. To, která ID uživatelů jsou kontrolována, závisí na používaném komunikačním protokolu a na nastavení atributu kanálu PUTAUT. Další informace viz “ID uživatelů používaná inicializátorem kanálu” na stránce 242.

Pokud jedno z těchto ID uživatelů nemá přístup k prostředku, požadavek selže s kódem dokončení MQRC_NOT_AUTHORIZED.

Jak může RESLEVEL ovlivnit provedené kontroly

V závislosti na tom, jak jste nastavili profil RESLEVEL, můžete změnit, která ID uživatelů jsou kontrolována, když je požadován přístup k prostředku, a kolik z nich je kontrolováno.

V následující tabulce jsou uvedeny kontroly provedené pro připojení inicializátoru kanálu a pro všechny kanály, které používají toto připojení.

Tabulka 55. Kontroly provedené na různých úrovních přístupu RACF pro připojení inicializátoru kanálu	
RACF úroveň přístupu	**Úroveň kontroly**
ŽÁDNÉ	Zkontrolujte dvě ID uživatelů.
READ (čtení)	Zkontrolujte jedno ID uživatele.
AKTUALIZOVAT	Zkontrolujte jedno ID uživatele.
CONTROL	Žádný šek.
ALTER	Žádný šek.
Poznámka: Definice kontrolovaných ID uživatelů viz “ID uživatelů používaná inicializátorem kanálu” na stránce 242 .	

z/OS *RESLEVEL a řazení do front v rámci skupiny*

Při výchozím nastavení, když agent front v rámci skupiny provádí kontrolu zabezpečení prostředku rozhraní API, jsou zkontrolována dvě ID uživatelů, aby se zjistilo, zda je k prostředku povolen přístup. Můžete změnit, která ID uživatelů se kontrolují, nastavením profilu RESLEVEL.

Kontrolovaná ID uživatelů mohou být ID uživatele určené atributem IGQUSER přijímajícího správce front, ID uživatele správce front v rámci skupiny sdílení front, která vložila zprávu do systému SYSTEM.QSG.TRANSMIT.QUEUEnebo alternativní ID uživatele uvedené v poli *UserIdentifier* deskriptoru zprávy zprávy. Další informace viz “ID uživatelů používaná agentem front v rámci skupiny” na stránce 246.

Vzhledem k tomu, že agent řazení do front v rámci skupiny je interní úlohou správce front, nevydá explicitní požadavek na připojení a spustí se pod ID uživatele správce front. Agent front v rámci skupiny se spouští při inicializaci správce front. Během inicializace agenta front v rámci skupiny produkt IBM MQ kontroluje přístup, který má ID uživatele přidružené ke správci front k profilu ve třídě MQADMIN s názvem:

```
hlq.RESLEVEL
```

Tato kontrola se provádí vždy, pokud není nastaven přepínač hlq.NO.SUBSYS.SECURITY .

Pokud neexistuje žádný profil RESLEVEL, produkt IBM MQ povolí kontrolu dvou ID uživatelů. Pokud existuje profil RESLEVEL, závisí úroveň kontroly na úrovni přístupu udělené ID uživatele správce front pro daný profil. Kontroly provedené na různých RACF(r) úrovních přístupu pro agenta front v rámci skupiny zobrazují kontroly provedené pro agenta front v rámci skupiny.

Tabulka 56. Kontroly provedené na různých úrovních přístupu RACF pro agenta front v rámci skupiny

RACF úroveň přístupu	**Úroveň kontroly**
ŽÁDNÉ	Zkontrolujte dvě ID uživatelů.
READ (čtení)	Zkontrolujte jedno ID uživatele.
AKTUALIZOVAT	Zkontrolujte jedno ID uživatele.
CONTROL	Žádný šek.
ALTER	Žádný šek.
Poznámka: Definice kontrolovaných ID uživatelů viz “ID uživatelů používaná agentem front v rámci skupiny” na stránce 246 .	

Pokud se změní oprávnění udělená profilu RESLEVEL pro ID uživatele správce front, je nutné zastavit a restartovat agenta řazení do fronty v rámci skupiny, aby se získala nová oprávnění. Vzhledem k tomu, že neexistuje žádný způsob, jak nezávisle zastavit a restartovat agenta řazení do fronty v rámci skupiny, je nutné zastavit a restartovat správce front, aby se toho dosáhlo.

z/OS *RESLEVEL a zkontrolována ID uživatelů*

Příklad nastavení profilu RESLEVEL a udělení přístupu k němu.

Kontrola ID uživatele podle názvu profilu pro dávková připojení prostřednictvím ID uživatele podle názvu profilu pro LU 6.2 a kanály připojení serveru TCP/IP ukazuje, jak RESLEVEL ovlivňuje, která ID uživatelů jsou kontrolována pro různé požadavky MQI.

Máte například správce front s názvem QM66 s následujícími požadavky:

- Uživatel WS21B má být vyloučen ze zabezpečení prostředků.
- CICS spuštěná úloha WXNCICS spuštěná pod ID uživatele adresního prostoru CICSWXN má provádět úplnou kontrolu prostředků pouze pro transakce definované s hodnotou RESSEC (YES).

Chcete-li definovat příslušný profil RESLEVEL, zadejte následující příkaz RACF :

```
RDEFINE MQADMIN QM66.RESLEVEL UACC(NONE)
```

Poté udělte uživatelům přístup k tomuto profilu pomocí následujících příkazů:

```
PERMIT QM66.RESLEVEL CLASS(MQADMIN) ID(WS21B) ACCESS(CONTROL)
PERMIT QM66.RESLEVEL CLASS(MQADMIN) ID(CICSWXN) ACCESS(UPDATE)
```

Provedete-li tyto změny v době, kdy jsou ID uživatelů připojena ke správci front QM66, musí se uživatelé před provedením změny odpojit a znovu připojit.

Pokud zabezpečení subsystému není aktivní, když se uživatel připojí, ale když je tento uživatel stále připojen, zabezpečení subsystému se stane aktivním, bude pro uživatele použita úplná kontrola zabezpečení prostředků. Uživatel se musí znovu připojit, aby získal správné zpracování RESLEVEL.

z/OS ID uživatelů pro kontrolu zabezpečení na systému z/OS

Produkt IBM MQ zahajuje kontroly zabezpečení na základě ID uživatelů přidružených k uživatelům, terminálům, aplikacím a dalším prostředkům. Tato kolekce témat uvádí, která ID uživatelů se používají pro každý typ kontroly zabezpečení.

z/OS *ID uživatelů pro zabezpečení připojení*

ID uživatele použité pro zabezpečení připojení závisí na typu připojení.

Typ připojení	Obsah ID uživatele
Dávkové připojení	ID uživatele připojující se úlohy. Příklad: • ID uživatele TSO • ID uživatele přiřazené dávkové úloze parametrem USER JCL • ID uživatele přiřazené ke spuštěné úloze třídou STARTED nebo tabulkou spuštěných procedur
CICS připojení	ID uživatele adresního prostoru CICS .
IMS připojení	ID uživatele adresního prostoru oblasti IMS .
Připojení inicializátoru kanálu	ID uživatele adresního prostoru inicializátoru kanálu.

z/OS *ID uživatelů pro zabezpečení příkazů a prostředků příkazů*

ID uživatele použité pro zabezpečení příkazů nebo zabezpečení prostředků příkazů závisí na tom, odkud byl příkaz zadán.

Vydáno od ...	Obsah ID uživatele
CSQINP1, CSQINP2nebo CSQINPT	Neprovádí se žádná kontrola.
Vstupní fronta systémových příkazů	ID uživatele nalezené v souboru *UserIdentifier* deskriptoru zprávy, který obsahuje příkaz. Pokud zpráva neobsahuje *UserIdentifier*, je správci zabezpečení předáno ID uživatele s mezerami.
Konzola	ID uživatele přihlášeného ke konzole. Pokud není konzola přihlášena, výchozí ID uživatele nastavené systémovým parametrem CMDUSER v CSQ6SYSP. Chcete-li zadat příkazy z konzoly, musí mít konzola atribut z/OS SYS AUTHORITY.
SDSF/Konzola TSO	TSO nebo ID uživatele úlohy.

Vydáno od ...	Obsah ID uživatele
Provozní a ovládací panely	ID uživatele TSO. Pokud se chystáte používat operace a ovládací panely, musíte mít odpovídající oprávnění k zadávání příkazů odpovídajících vámi zvoleným akcím. Kromě toho musíte mít přístup READ ke všem funkcím hlq.DISPLAY. Profily *objektu* ve třídě MQCMDS, protože panely používají různé příkazy DISPLAY ke shromáždění informací, které představují.
MGCRE	Pokud se MGCRE používá s UTOKEN, ID uživatele v UTOKEN. Pokud je MGCRE vydán bez UTOKEN, použije se TSO nebo ID uživatele úlohy.
CSQ0UTIL	ID uživatele úlohy.
CSQUTIL	ID uživatele úlohy.
CSQINPX	ID uživatele adresního prostoru inicializátoru kanálu.

z/OS *ID uživatelů pro zabezpečení prostředků (MQOPEN, MQSUB a MQPUT1)*

Tyto informace zobrazují obsah ID uživatelů pro normální a alternativní ID uživatelů pro každý typ připojení. Počet kontrol je definován profilem RESLEVEL. Kontrolované ID uživatele se používá pro volání **MQOPEN**, **MQSUB**nebo **MQPUT1** .

Poznámka: Všechna pole ID uživatele jsou kontrolována přesně tak, jak jsou přijímána. Neproběhnou žádné převody a například tři pole ID uživatele obsahující "Bob", "BOB"a "bob" nejsou ekvivalentní.

z/OS *ID uživatelů zaškrtnutá pro dávková připojení*

ID uživatele kontrolované pro dávkové připojení závisí na způsobu spuštění úlohy a na tom, zda bylo zadáno alternativní ID uživatele.

Tabulka 57. Kontrola ID uživatele podle názvu profilu pro dávková připojení

Alternativní ID uživatele zadané při otevření?	hlq.ALTERNATE.USER.userid	Profil hlq.CONTEXT.queuename	Profil hlq.resourcename
Ne	-	Úloha	Úloha
Ano	Úloha	Úloha	ALT

Klíč:

ALT
Alternativní ID uživatele.

Úloha

- ID uživatele přihlášení TSO nebo z/OS UNIX System Services .
- ID uživatele přiřazené dávkové úloze.
- ID uživatele přiřazené ke spuštěné úloze třídou STARTED nebo tabulkou spuštěných procedur.
- ID uživatele přidružené k prováděné uložené proceduře Db2

Dávková úloha provádí MQPUT1 do fronty s názvem Q1 s volbou RESLEVEL nastavenou na hodnotu READ a s vypnutou kontrolou alternativního ID uživatele.

Kontroly provedené na různých úrovních přístupu RACF(r) pro dávková připojení a ID uživatele kontrolující název profilu pro dávková připojení ukazují, že ID uživatele úlohy je kontrolováno podle profilu hlq.Q1.

z/OS *ID uživatelů zaškrtnutá pro připojení CICS*

ID uživatelů, která jsou kontrolována pro připojení produktu CICS , závisí na tom, zda se má provést jedna nebo dvě kontroly, a zda je zadáno alternativní ID uživatele.

Tabulka 58. Kontrola ID uživatele podle názvu profilu pro ID uživatele typu CICS

Alternativní ID uživatele zadané při otevření?	hlq.ALTERNATE.USER.userid	Profil hlq.CONTEXT.queuename	Profil hlq.resourcename
Ne, 1 kontrola	-	ADS	ADS
Ne, 2 kontroly	-	ADS + TXN	ADS + TXN
Ano, 1 kontrola	ADS	ADS	ADS
Ano, 2 kontroly	ADS + TXN	ADS + TXN	ADS + ALT

Klíč:

ALT
Jméno alternativního uživatele

ADS
ID uživatele přidružené k dávkové úloze CICS , nebo pokud je produkt CICS spuštěn jako spuštěná úloha, prostřednictvím třídy STARTED nebo tabulky spuštěných procedur.

TXN
ID uživatele přidružené k transakci CICS . Toto je obvykle ID uživatele terminálu, který spustil transakci. Může to být CICS DFLTUSER, terminál zabezpečení PRESET nebo ručně přihlášený uživatel.

Určete ID uživatelů, u kterých byla provedena kontrola za následujících podmínek:

- Úroveň přístupu RACF k profilu RESLEVEL pro ID uživatele adresního prostoru CICS je nastavena na hodnotu NONE.
- Volání MQOPEN je provedeno pro frontu s MQOO_OUTPUT a MQOO_PASS_IDENTITY_CONTEXT.

Nejprve se podívejte, kolik ID uživatelů produktu CICS je kontrolováno na základě přístupu ID uživatele adresního prostoru CICS k profilu RESLEVEL. V části Tabulka 53 na stránce 236 v tématu “RESLEVEL a CICS připojení” na stránce 235jsou zaškrtnuta dvě ID uživatelů, pokud je profil RESLEVEL nastaven na hodnotu NONE. Poté, od Tabulka 58 na stránce 241 na, tyto kontroly se provádějí:

- Pole hlq.ALTERNATE.USER.userid není kontrolován.
- Profil hlq.CONTEXT.queuename se kontroluje na ID uživatele adresního prostoru CICS a ID uživatele transakce CICS .
- Profil hlq.resourcename je kontrolován jak ID uživatele adresního prostoru CICS , tak ID uživatele transakce CICS .

To znamená, že pro toto volání MQOPEN jsou provedeny čtyři kontroly zabezpečení.

z/OS *ID uživatelů zaškrtnutá pro připojení IMS*

ID uživatelů kontrolovaná pro připojení produktu IMS závisí na tom, zda se má provést jedna nebo dvě kontroly a zda je zadáno alternativní ID uživatele. Je-li zaškrtnuto druhé ID uživatele, závisí na typu závislé oblasti a na tom, která ID uživatelů jsou k dispozici.

Tabulka 59. Kontrola ID uživatele podle názvu profilu pro ID uživatele typu IMS

Alternativní ID uživatele zadané při otevření?	hlq.ALTERNATE.USER.userid	Profil hlq.CONTEXT.queuename	Profil hlq.resourcename
Ne, 1 kontrola	-	REG	REG
Ne, 2 kontroly	-	REG + SEC	REG + SEC

Tabulka 59. Kontrola ID uživatele podle názvu profilu pro ID uživatele typu IMS (pokračování)			
Alternativní ID uživatele zadané při otevření?	**hlq.ALTERNATE.USER.userid**	**Profil hlq.CONTEXT.queuename**	**Profil hlq.resourcename**
Ano, 1 kontrola	REG	REG	REG
Ano, 2 kontroly	REG + SEC	REG + SEC	REG + ALT

Klíč:

ALT
Alternativní ID uživatele.

REG
ID uživatele je obvykle nastaveno prostřednictvím třídy STARTED nebo tabulky spuštěných procedur, nebo pokud je spuštěn IMS , z odeslané úlohy pomocí parametru USER JCL.

Sek
Druhé ID uživatele je přidruženo k práci, která se provádí v závislé oblasti. Určuje se podle Tabulka 60 na stránce 242.

Tabulka 60. Jak je určeno druhé ID uživatele pro připojení IMS	
Typy závislých oblastí	**Hierarchie pro určení druhého ID uživatele**
• Byla vydána zpráva řízená BMP a úspěšná operace GET UNIQUE. • Byl vydán příkaz IFP a GET UNIQUE. • MPP.	ID uživatele přidružené k transakci IMS , pokud je uživatel přihlášen. Název LTERM, je-li k dispozici. PSBNAME.
• Zpráva řízená BMP a úspěšná operace GET UNIQUE nebyla vydána. • BMP není řízen zprávami. • IFP a GET UNIQUE nebyly vydány.	ID uživatele přidružené k adresnímu prostoru závislé oblasti IMS , pokud se nejedná o všechny mezery nebo nuly. PSBNAME.

z/OS *ID uživatelů používaná inicializátorem kanálu*

Tato kolekce témat popisuje ID uživatelů používaná a kontrolovaná pro přijímací kanály a pro požadavky MQI klienta vydané prostřednictvím kanálů připojení serveru. Informace jsou poskytovány pro TCP/IP a pro LU6.2

K určení použitého typu kontroly zabezpečení můžete použít parametr PUTAUT definice přijímacího kanálu. Chcete-li získat konzistentní kontrolu zabezpečení v celé síti IBM MQ , můžete použít volby ONLYMCA a ALTMCA.

Pomocí příkazu DISPLAY CHSTATUS můžete určit identifikátor uživatele používaný agentem MCA.

z/OS *Příjem kanálů používajících protokol TCP/IP*

Kontrolovaná ID uživatelů závisí na volbě PUTAUT kanálu a na tom, zda se má provést jedna nebo dvě kontroly.

Tabulka 61. ID uživatelů, která byla zkontrolována proti názvu profilu pro kanály TCP/IP			
V kanálu příjemce nebo žadatele byla zadána volba PUTAUT.	**hlq.ALTERNATE.USER.userid**	**Profil hlq.CONTEXT.queuename**	**Profil hlq.resourcename**
DEF, 1 kontrola	-	CHL	CHL

Tabulka 61. ID uživatelů, která byla zkontrolována proti názvu profilu pro kanály TCP/IP (pokračování)			
V kanálu příjemce nebo žadatele byla zadána volba PUTAUT.	**hlq.ALTERNATE.USER.userid**	**Profil hlq.CONTEXT.queuename**	**Profil hlq.resourcename**
DEF, 2 kontroly	-	CHL + MCA-základní	CHL + MCA-základní
CTX, 1 kontrola	CHL	CHL	CHL
CTX, 2 kontroly	CHL + MCA-základní	CHL + MCA-základní	CHL + ALT
ONLYMCA, 1 kontrola	-	MCA	MCA
ONLYMCA, 2 kontroly	-	MCA	MCA
ALTMCA, 1 kontrola	MCA	MCA	MCA
ALTMCA, 2 kontroly	MCA	MCA	MCA + ALT

Klíč:

MCA (ID uživatele MCA)
ID uživatele uvedené pro atribut kanálu MCAUSER na přijímači; pokud je prázdné, použije se ID uživatele adresního prostoru inicializátoru kanálu na straně příjemce nebo žadatele.

CHL (ID uživatele kanálu)
V případě protokolu TCP/IP není zabezpečení pro kanál podporováno komunikačním systémem. Pokud se používá protokol TLS (Transport Layer Security) a od partnera byl vydán digitální certifikát, použije se ID uživatele přidružené k tomuto certifikátu (je-li nainstalován) nebo ID uživatele přidružené k odpovídajícímu filtru nalezenému pomocí CNF (RACF Certificate Name Filtering). Není-li nalezeno žádné přidružené ID uživatele nebo není-li použito zabezpečení TLS, použije se jako ID uživatele kanálu v kanálech definovaných s parametrem PUTAUT nastaveným na hodnotu DEF nebo CTX ID uživatele inicializátoru kanálu adresního prostoru příjemce nebo konce žadatele.

Poznámka: Použití CNF (RACF Certificate Name Filtering) vám umožňuje přiřadit stejné ID uživatele RACF více vzdáleným uživatelům, například všem uživatelům ve stejné organizační jednotce, kteří by přirozeně měli stejnou bezpečnostní autoritu. To znamená, že server nemusí mít kopii certifikátu všech možných vzdálených uživatelů po celém světě a výrazně zjednodušuje správu a distribuci certifikátů.

Je-li parametr PUTAUT pro kanál nastaven na hodnotu ONLYMCA nebo ALTMCA, bude jméno uživatele kanálu ignorováno a bude použito jméno uživatele MCA příjemce nebo žadatele. To platí i pro kanály TCP/IP používající protokol TLS.

ALT (Alternativní ID uživatele)
ID uživatele z informací o kontextu (tj. pole *UserIdentifier*) v deskriptoru zprávy. Toto ID uživatele je přesunuto do pole *AlternateUserID* v deskriptoru objektu před vydáním volání **MQOPEN** nebo **MQPUT1** pro cílovou frontu.

z/OS *Příjem kanálů pomocí LU 6.2*

Kontrolovaná ID uživatelů závisí na volbě PUTAUT kanálu a na tom, zda se má provést jedna nebo dvě kontroly.

Tabulka 62. ID uživatelů ověřených podle jména profilu pro kanály LU 6.2			
V kanálu příjemce nebo žadatele byla zadána volba PUTAUT.	**hlq.ALTERNATE.USER.userid**	**Profil hlq.CONTEXT.queuename**	**Profil hlq.resourcename**
DEF, 1 kontrola	-	CHL	CHL
DEF, 2 kontroly	-	CHL + MCA-základní	CHL + MCA-základní
CTX, 1 kontrola	CHL	CHL	CHL
CTX, 2 kontroly	CHL + MCA-základní	CHL + MCA-základní	CHL + ALT
ONLYMCA, 1 kontrola	-	MCA	MCA
ONLYMCA, 2 kontroly	-	MCA	MCA
ALTMCA, 1 kontrola	MCA	MCA	MCA
ALTMCA, 2 kontroly	MCA	MCA	MCA + ALT

Klíč:

MCA (ID uživatele MCA)
ID uživatele uvedené pro atribut kanálu MCAUSER na přijímači; pokud je prázdné, použije se ID uživatele adresního prostoru inicializátoru kanálu na straně příjemce nebo žadatele.

CHL (ID uživatele kanálu)

Kanály žadatele-server
Je-li kanál spuštěn od žadatele, není možné přijmout ID uživatele sítě (ID uživatele kanálu).

Je-li parametr PUTAUT nastaven na hodnotu DEF nebo CTX v žadatelském kanálu, je ID uživatele kanálu adresním prostorem inicializátoru kanálu žadatele, protože ze sítě nebylo přijato žádné ID uživatele.

Pokud je parametr PUTAUT nastaven na ONLYMCA nebo ALTMCA, ID uživatele kanálu se ignoruje a použije se ID uživatele MCA žadatele.

Jiné typy kanálů
Je-li parametr PUTAUT nastaven na hodnotu DEF nebo CTX v kanálu příjemce nebo žadatele, ID uživatele kanálu je ID uživatele přijaté z komunikačního systému při zahájení kanálu.

- Pokud je odesílající kanál v systému z/OS, přijaté ID uživatele kanálu je ID uživatele adresního prostoru inicializátoru kanálu odesilatele.
- Pokud je odesílající kanál na jiné platformě (například AIX), je přijaté ID uživatele kanálu obvykle poskytnuto parametrem USERID definice kanálu.

Pokud je přijaté ID uživatele prázdné nebo není přijato žádné ID uživatele, použije se ID uživatele kanálu s mezerami.

ALT (Alternativní ID uživatele)
ID uživatele z informací o kontextu (tj. pole *UserIdentifier*) v deskriptoru zprávy. Toto ID uživatele je přesunuto do pole *AlternateUserID* v deskriptoru objektu před vydáním volání MQOPEN nebo MQPUT1 pro cílovou frontu.

z/OS *Požadavky MQI klienta*
Lze použít různá ID uživatelů v závislosti na tom, která ID uživatelů a proměnné prostředí byly nastaveny. Tato ID uživatelů jsou kontrolována pro různé profily v závislosti na použité volbě PUTAUT a na tom, zda je zadáno alternativní ID uživatele.

Tato část popisuje ID uživatelů, která jsou kontrolována pro požadavky MQI klienta vydané prostřednictvím kanálů připojení serveru pro protokol TCP/IP a LU 6.2. ID uživatele MCA a ID uživatele kanálu jsou stejné jako pro kanály TCP/IP a LU 6.2 popsané v předchozích sekcích.

Pro kanály připojení serveru se použije ID uživatele přijaté od klienta, pokud je atribut MCAUSER prázdný.

Další informace viz “Řízení přístupu pro klienty” na stránce 102.

Pro požadavky klienta **MQOPEN**, **MQSUB**a **MQPUT1** použijte následující pravidla k určení profilu, který je kontrolován:

- Pokud požadavek uvádí oprávnění alternativního uživatele, provede se kontrola na *hlq*.ALTERNATE.USER. Profil *userid* .
- Pokud požadavek uvádí kontextové oprávnění, provede se kontrola na *hlq*.KONTEXT. Profil *queuename* .
- Pro všechny požadavky **MQOPEN**, **MQSUB**a **MQPUT1** se provede kontrola profilu *hlq.resourcename* .

Po zjištění, které profily jsou kontrolovány, použijte následující tabulku k určení, která ID uživatelů jsou kontrolována proti těmto profilům.

Tabulka 63. ID uživatelů ověřených podle názvu profilu pro kanály připojení serveru LU 6.2 a TCP/IP

V kanálu připojení serveru byla zadána volba PUTAUT.	Alternativní ID uživatele zadané při otevření?	hlq.ALTERNATE.USER.userid	Profil hlq.CONTEXT.queuename	Profil hlq.resourcename
DEF, 1 kontrola	Ne	-	CHL	CHL
DEF, 1 kontrola	Ano	CHL	CHL	CHL
DEF, 2 kontroly	Ne	-	CHL + MCA-základní	CHL + MCA-základní
DEF, 2 kontroly	Ano	CHL + MCA-základní	CHL + MCA-základní	CHL + ALT
ONLYMCA, 1 kontrola	Ne	-	MCA	MCA
ONLYMCA, 1 kontrola	Ano	MCA	MCA	MCA
ONLYMCA, 2 kontroly	Ne	-	MCA	MCA
ONLYMCA, 2 kontroly	Ano	MCA	MCA	MCA + ALT

Klíč:

MCA (ID uživatele MCA)
ID uživatele zadané pro atribut kanálu MCAUSER v připojení k serveru; je-li prázdné, použije se ID uživatele adresního prostoru inicializátoru kanálu.

CHL (ID uživatele kanálu)
V případě protokolu TCP/IP není zabezpečení pro kanál podporováno komunikačním systémem. Pokud se používá protokol TLS (Transport Layer Security) a od partnera byl vydán digitální certifikát, použije se ID uživatele přidružené k tomuto certifikátu (je-li nainstalován) nebo ID uživatele přidružené k odpovídajícímu filtru nalezenému pomocí CNF (RACF Certificate Name Filtering).

Není-li nalezeno žádné přidružené ID uživatele nebo není-li použito zabezpečení TLS, použije se ID uživatele adresního prostoru inicializátoru kanálu jako ID uživatele kanálu na kanálech definovaných s parametrem PUTAUT nastaveným na hodnotu DEF nebo CTX.

Poznámka: Použití CNF (RACF Certificate Name Filtering) vám umožňuje přiřadit stejné ID uživatele RACF více vzdáleným uživatelům, například všem uživatelům ve stejné organizační jednotce, kteří by přirozeně měli stejnou bezpečnostní autoritu. To znamená, že server nemusí mít kopii certifikátu všech možných vzdálených uživatelů po celém světě a výrazně zjednodušuje správu a distribuci certifikátů.

Je-li parametr PUTAUT pro kanál nastaven na hodnotu ONLYMCA nebo ALTMCA, bude jméno uživatele kanálu ignorováno a bude použito jméno uživatele MCA kanálu připojení serveru. To platí i pro kanály TCP/IP používající protokol TLS.

ALT (Alternativní ID uživatele)
ID uživatele z informací o kontextu (tj. pole *UserIdentifier*) v deskriptoru zprávy. Toto ID uživatele je přesunuto do pole *AlternateUserID* v objektu nebo deskriptoru odběru před vydáním volání **MQOPEN**, **MQSUB** nebo **MQPUT1** jménem klientské aplikace.

z/OS *Příklad inicializátoru kanálu*

Příklad toho, jak jsou ID uživatelů kontrolována proti profilům RACF .

Uživatel provede operaci **MQPUT1** pro frontu ve správci front QM01 , která se interpretuje jako fronta s názvem QB ve správci front QM02. Zpráva je odeslána prostřednictvím kanálu TCP/IP s názvem QM01.TO.QM02. RESLEVEL je nastaven na NONE a otevření se provádí s alternativním ID uživatele a kontrolou kontextu. Definice kanálu příjemce má PUTAUT (CTX) a je nastaveno ID uživatele MCA. Která ID uživatelů se používají v přijímacím kanálu pro vložení zprávy do fronty QB?

Odpověď: Tabulka 55 na stránce 237 ukazuje, že jsou zaškrtnuta dvě ID uživatelů, protože parametr RESLEVEL je nastaven na hodnotu NONE.

Tabulka 61 na stránce 242 ukazuje, že s PUTAUT nastaveným na CTX a 2 kontrolami jsou kontrolována následující ID uživatelů:

- ID uživatele inicializátoru kanálu a ID uživatele MCAUSER jsou kontrolovány proti hlq.ALTERNATE.USER.userid .
- ID uživatele inicializátoru kanálu a ID uživatele MCAUSER jsou kontrolovány proti profilu hlq.CONTEXT.queuename .
- ID uživatele inicializátoru kanálu a alternativní ID uživatele zadané v deskriptoru zpráv (MQMD) jsou kontrolovány podle profilu hlq.Q2 .

z/OS *ID uživatelů používaná agentem front v rámci skupiny*

Jména uživatelů, která jsou kontrolována při otevření cílových front agentem front v rámci skupiny, jsou určena hodnotami atributů správce front **IGQAUT** a **IGQUSER** .

Možná ID uživatelů jsou:

ID uživatele řazení do front v rámci skupiny (IGQ)
ID uživatele určené atributem **IGQUSER** přijímajícího správce front. Je-li tato volba nastavena na mezery, použije se ID uživatele přijímajícího správce front. Avšak vzhledem k tomu, že přijímající správce front má oprávnění pro přístup ke všem definovaným frontám, kontroly zabezpečení se neprovádějí pro ID uživatele přijímajícího správce front. V tomto případě:

- Má-li být zkontrolováno pouze jedno ID uživatele a ID uživatele je ID přijímajícího správce front, nebudou provedeny žádné kontroly zabezpečení. K tomu může dojít, je-li parametr **IGQAUT** nastaven na hodnotu ONLYIGQ nebo ALTIGQ.
- Mají-li být zkontrolována dvě ID uživatelů a jedno z ID uživatelů je ID přijímajícího správce front, budou provedeny kontroly zabezpečení pouze pro ostatní ID uživatelů. K tomu může dojít, když je parametr **IGQAUT** nastaven na hodnotu DEF, CTXnebo ALTIGQ.

- Mají-li být zkontrolována dvě ID uživatelů a obě ID uživatelů jsou ID přijímajícího správce front, nebudou provedeny žádné kontroly zabezpečení. K tomu může dojít, když je parametr **IGQAUT** nastaven na hodnotu ONLYIGQ.

Odesílání ID uživatele správce front (SND)
ID uživatele správce front ve skupině sdílení front, která vložila zprávu do systému SYSTEM.QSG.TRANSMIT.QUEUE.

Alternativní ID uživatele (ALT)
ID uživatele uvedené v poli *UserIdentifier* v deskriptoru zprávy zprávy.

Tabulka 64. ID uživatelů, která byla zkontrolována proti názvu profilu pro řazení do fronty v rámci skupiny

Volba IGQAUT zadaná v přijímajícím správci front	hlq.ALTERNATE.USER.userid	Profil hlq.CONTEXT.queuename	Profil hlq.resourcename
DEF, 1 kontrola	-	SND	SND
DEF, 2 kontroly	-	SND + IGQ	SND + IGQ
CTX, 1 kontrola	SND	SND	SND
CTX, 2 kontroly	SND + IGQ	SND + IGQ	SND + ALT
ONLYIGQ, 1 kontrola	-	IGQ	IGQ
ONLYIGQ, 2 kontroly	-	IGQ	IGQ
ALTIGQ, 1 kontrola	-	IGQ	IGQ
ALTIGQ, 2 kontroly	IGQ	IGQ	IGQ + ALT

Klíč:

ALT
Alternativní ID uživatele.

IGQ
ID uživatele IGQ.

SND
Probíhá odesílání ID uživatele správce front.

z/OS *Prázdná ID uživatelů a úrovně UACC*

Pokud se vyskytne prázdné ID uživatele, je přihlášen RACF nedefinovaný uživatel. Neudělujte nedefinovanému uživateli rozsáhlý přístup.

Prázdná ID uživatelů mohou existovat, když uživatel manipuluje se zprávami pomocí kontextu nebo zabezpečení alternativního uživatele, nebo když je produktu IBM MQ předáno prázdné ID uživatele. Prázdné ID uživatele se například použije, když je zpráva zapsána do vstupní fronty systémového příkazu bez kontextu.

Poznámka: ID uživatele " * " (tj. znak hvězdičky následovaný sedmi mezerami) je považován za nedefinované ID uživatele.

Produkt IBM MQ předá prázdné ID uživatele do produktu RACF a RACF nedefinovaný uživatel je přihlášen. Všechny bezpečnostní kontroly pak používají univerzální přístup (UACC) pro příslušný profil. V závislosti na tom, jak jste nastavili úrovně přístupu, může UACC poskytnout nedefinovanému uživateli široký přístup.

Pokud například zadáte tento příkaz RACF z TSO:

```
RDEFINE MQQUEUE Q.AVAILABLE.TO.EVERYONE UACC(UPDATE)
```

Definujete profil, který umožňuje, aby ID uživatele definovaná v systému z/OS(která nebyla vložena do seznamu pro přístup) a nedefinované ID uživatele systému RACF vkládaly zprávy do této fronty a získalo zprávy z této fronty.

Chcete-li chránit před prázdnými ID uživatelů, musíte pečlivě naplánovat úrovně přístupu a omezit počet osob, které mohou používat kontext a zabezpečení alternativního uživatele. Lidem, kteří používají nedefinované ID uživatele RACF , musíte zabránit v získání přístupu k prostředkům, ke kterým nemají přístup. Současně však musíte povolit přístup k osobám s definovanými ID uživatelů. Chcete-li to provést, můžete zadat ID uživatele s hvězdičkou (*) v příkazu RACF PERMIT a poskytnout přístup k prostředkům pro všechna definovaná ID uživatelů. Proto všechna nedefinovaná ID uživatelů (například " * ") je odepřen přístup. Například tyto příkazy RACF brání nedefinovanému ID uživatele RACF v získání přístupu k frontě pro vložení nebo získání zpráv:

```
RDEFINE MQQUEUE Q.AVAILABLE.TO.RACF.DEFINED.USERS.ONLY UACC(NONE)
PERMIT Q.AVAILABLE.TO.RACF.DEFINED.USERS.ONLY CLASS(MQQUEUE) ACCESS(UPDATE) ID(*)
```

z/OS z/OS ID uživatelů a vícefaktorové ověření (MFA)

Volba IBM Vícefaktorové ověřování pro produkt z/OS umožňuje administrátorům zabezpečení produktu z/OS rozšířit ověřování SAF tím, že od identifikovaných uživatelů vyžaduje použití více ověřovacích faktorů (například heslo i šifrovací token) pro přihlášení k systému z/OS . IBM MFA také poskytuje podporu pro technologie generování jednorázových hesel založených na čase, jako např. RSA SecureId.

Z větší části produkt IBM MQ neví, jak se uživatelé "přihlásili" k systému CICS nebo dávkovým systémům, které řídí práci IBM MQ , přihlašovací pověření ID uživatele je přidruženo k úloze z/OS nebo adresnímu prostoru a produkt IBM MQ toto používá ke kontrole autorizace k prostředkům. ID uživatelů povolená pro vícenásobné ověření lze použít pro autorizaci k prostředkům IBM MQ a ověření přes průchozí tikety použité s mosty CICS a IMS .

Důležité: Při použití aplikací, jako např. IBM MQ Explorer, které předávají pověření ID uživatele a hesla pro volání MQCONNX API s volbou *MQCSP_AUTH_USER_ID_AND_PWD* , však platí zvláštní aspekty. Produkt IBM MQ nemá žádné zařízení pro předání dalšího pověření pro tento požadavek rozhraní API.

Omezení a možná náhradní řešení jsou popsána v následujícím textu.

IBM MQ Explorer

IBM MQ Explorer nelze použít pro přihlášení k systému z/OS s ID uživatele, pro které je MFA povoleno, protože neexistuje prostředek pro předání druhého ověřovacího faktoru z IBM MQ Explorer do z/OS.

Kromě toho existují dva různé mechanizmy používané produktem IBM MQ Explorer k opětovnému použití pověření ID uživatele a hesla, které vyžadují zvláštní pozornost, když jsou jednorázová hesla v platnosti:

1. Produkt IBM MQ Explorer má možnost ukládat hesla v zakrytém formátu na lokálním počítači pro pozdější přihlášení. Tato schopnost musí být zakázána tak, že se při každém připojení ke správci front z/OS zobrazí výzva k zadání hesla průzkumníka.

   Chcete-li to provést, postupujte takto:

   a. Vyberte volbu **Správci front**.

   b. Ze zobrazeného seznamu vyberte požadovaného správce front a klepněte na něj pravým tlačítkem myši.

   c. V zobrazeném seznamu nabídky vyberte volbu **Podrobnosti připojení** .

   d. V dalším seznamu nabídky vyberte volbu **Vlastnosti** a vyberte kartu **ID uživatele** .

      Ujistěte se, že jste vybrali přepínač **výzva k zadání hesla** .

2. Různé operace v produktu IBM MQ Explorer, například procházení zpráv ve frontách, testování odběrů atd., spustí nový podproces, který se ověří v produktu IBM MQ pomocí pověření, které bylo poprvé použito při přihlášení. Protože pověření heslem nelze znovu použít, nemůžete tyto operace použít.

Existují dvě možná náhradní řešení na úrovni konfigurace MFA pro tyto problémy:

- Použijte vyloučení ID aplikace vícenásobného ověření, abyste úplně vyloučili úlohy IBM MQ ze zpracování vícenásobného ověření.

  Chcete-li to provést, zadejte následující příkazy:

  1. ```
     RDEFINE MFADEF MFABYPASS.USERID.chinuser
     ```

     kde *chinuser* je ID uživatele úrovně adresního prostoru inicializátoru kanálu (přidružené k inicializátoru kanálu prostřednictvím třídy STC)

  2. ```
     PERMIT MFABYPASS.USERID.chinuser CLASS MFADEF ACCESS(READ) ID(explorer user)
     ```

  Další informace o tomto přístupu naleznete v tématu Vynechání IBM MFA pro aplikace.
- Použijte podporu typu out-of-band na MFA, která byla zavedena s IBM MFA 1.2. Pomocí tohoto přístupu se předběžně ověřujete na webovém serveru IBM MFA a kromě ID uživatele a hesla uveďte další ověření, jak je určeno prostřednictvím zásady. IBM MFA server vygeneruje pověření tokenu mezipaměti, které pak zadáte v dialogovém okně ověření IBM MQ Explorer . Administrátor zabezpečení může povolit přehrání tohoto pověření po přiměřenou dobu, takže povolí normální použití produktu IBM MQ Explorer .

Další informace o tomto přístupu viz Úvod do produktu IBM MFA.

z/OS IBM MQ for z/OS správa zabezpečení

Produkt IBM MQ používá tabulku v úložišti k uchování informací souvisejících s každým uživatelem a požadavky na přístup každého uživatele. Chcete-li tuto tabulku spravovat efektivně a snížit počet požadavků provedených z produktu IBM MQ na externího správce zabezpečení (ESM), je k dispozici řada ovládacích prvků.

Tyto ovládací prvky jsou k dispozici jak prostřednictvím operací, tak prostřednictvím ovládacích panelů a příkazů IBM MQ .

z/OS *Opětovné vrácení ID uživatele*

Pokud byla změněna definice RACF uživatele, který používá prostředky IBM MQ , například připojením uživatele k nové skupině, můžete správci front sdělit, aby podepsal tohoto uživatele znovu při příštím pokusu o přístup k prostředku IBM MQ . To lze provést pomocí příkazu IBM MQ RVERIFY SECURITY.

- Uživatel HX0804 získává a vkládá zprávy do front PAYROLL ve správci front PRD1. Produkt HX0804 však nyní vyžaduje přístup k některým frontám PENSION ve stejném správci front (PRD1).
- Administrátor zabezpečení dat připojí uživatele HX0804 ke skupině RACF , která umožňuje přístup k frontám PENSION.
- Aby mohl produkt HX0804 přistupovat k frontám PENSION okamžitě (tj. bez ukončení práce správce front PRD1 nebo bez čekání na časový limit HX0804), musíte použít příkaz IBM MQ :

```
RVERIFY SECURITY(HX0804)
```

Poznámka: Pokud při spuštění správce front vypnete časový limit ID uživatele na dlouhá časová období (dny nebo dokonce týdny), nezapomeňte spustit příkaz RVERIFY SECURITY pro všechny uživatele, kteří byli v této době odvoláni nebo odstraněni.

z/OS *Vypršení časového limitu ID uživatele*

Po určité době nečinnosti můžete uživatele IBM MQ odhlásit od správce front.

Když uživatel přistupuje k prostředku IBM MQ , pokusí se správce front přihlásit tohoto uživatele ke správci front (pokud je zabezpečení subsystému aktivní). To znamená, že uživatel je ověřen v ESM. Tento uživatel zůstane přihlášen k produktu IBM MQ , dokud nebude správce front vypnut nebo dokud nebude ID uživatele *vypršel časový limit* (vypršení platnosti ověření) nebo nebude znovu ověřen (znovu ověřen).

Po vypršení časového limitu uživatele je ID uživatele *odhlášeno* v rámci správce front a veškeré informace související se zabezpečením uchovávané pro tohoto uživatele jsou zahozeny. Přihlášení a odhlášení uživatele v rámci správce front není pro aplikační program ani pro uživatele zřejmé.

Uživatelé jsou způsobilí k vypršení časového limitu, pokud nepoužili žádné prostředky IBM MQ po předem stanovenou dobu. Toto časové období je nastaveno příkazem MQSC ALTER SECURITY.

V příkazu ALTER SECURITY lze zadat dvě hodnoty:

TIMEOUT
Časové období v minutách, po které může nepoužívané ID uživatele a přidružené prostředky zůstat ve správci front IBM MQ .

INTERVAL
Časové období v minutách mezi kontrolami ID uživatelů a jejich přidruženými prostředky, které určuje, zda vypršela platnost *TIMEOUT* .

Je-li například hodnota *TIMEOUT* 30 a hodnota *INTERVAL* je 10, každých 10 minut IBM MQ zkontroluje ID uživatelů a jejich přidružené prostředky a určí, zda nebyly použity 30 minut. Pokud je nalezeno ID uživatele, jehož časový limit vypršel, je toto ID uživatele odhlášeno v rámci správce front. Pokud jsou nalezeny jakékoli informace o prostředku s vypršeným časovým limitem přidružené k ID uživatelů bez časového limitu, tyto informace o prostředku se vyřadí. Pokud nechcete, aby časový limit ID uživatelů uplynul, nastavte hodnotu *INTERVAL* na nulu. Je-li však hodnota *INTERVAL* nula, úložiště obsazené ID uživatelů a jejich přidružené prostředky se neuvolní, dokud nezadáte příkaz **REFRESH SECURITY** nebo **RVERIFY SECURITY** .

Vyladění této hodnoty může být důležité, pokud máte mnoho jednorázových uživatelů. Nastavíte-li malé hodnoty intervalu a časového limitu, prostředky, které již nejsou požadovány, se uvolní.

Poznámka: Pokud použijete jiné hodnoty pro *INTERVAL* nebo *TIMEOUT* než výchozí, musíte příkaz zadat znovu při každém spuštění správce front. To lze provést automaticky zadáním příkazu **ALTER SECURITY** do datové sady CSQINP1 pro daného správce front.

z/OS *Aktualizace zabezpečení správce front v systému z/OS*

IBM MQ for z/OS ukládá RACF data do mezipaměti, aby se zlepšil výkon. Při změně určitých tříd zabezpečení je nutné aktualizovat tyto informace uložené v mezipaměti. Z důvodu výkonu nepravidelně obnovujte zabezpečení. Můžete se také rozhodnout aktualizovat pouze informace o zabezpečení TLS.

Při prvním otevření fronty (nebo poprvé od aktualizace zabezpečení) produkt IBM MQ provede kontrolu RACF , aby získal přístupová práva uživatele, a umístí tyto informace do mezipaměti. Data uložená v mezipaměti zahrnují ID uživatelů a prostředky, na kterých byla provedena kontrola zabezpečení. Pokud je fronta znovu otevřena stejným uživatelem, přítomnost dat uložených v mezipaměti znamená, že IBM MQ nemusí vydávat RACF kontroly, což zlepšuje výkon. Akcí aktualizace zabezpečení je vyřadit veškeré informace o zabezpečení uložené v mezipaměti, a proto vynutit IBM MQ provedení nové kontroly proti RACF. Kdykoli přidáte, změníte nebo odstraníte profil prostředku RACF , který je zadržen ve třídě MQADMIN, MXADMIN, MQPROC, MXPROC, MQQUEUE, MXQUEUE, MQNLIST, MXNLIST nebo MXTOPIC, musíte správcům front, kteří používají tuto třídu, sdělit, aby aktualizovali informace o zabezpečení, které drží. Chcete-li to provést, zadejte následující příkazy:

- Příkaz RACF SETROPTS RACLIST (classname) REFRESH pro aktualizaci na úrovni RACF .
- Příkaz IBM MQ REFRESH SECURITY aktualizuje informace o zabezpečení uchovávané správcem front. Tento příkaz musí být zadán každým správcem front, který přistupuje ke změněným profilům. Máte-li skupinu sdílení front, můžete použít atribut oboru příkazu k nasměrování příkazu na všechny správce front ve skupině.

  Poznámka: Pokud jste připojili nového uživatele k existující skupině, musíte spustit příkaz IBM MQ RVERIFY SECURITY(userid). Příkaz REFRESH SECURITY (*) nedovolí, aby správce front znovu podepsal tohoto uživatele, a to při dalším pokusu o přístup k prostředku IBM MQ .

Pokud používáte generické profily v libovolné třídě IBM MQ , musíte také vydat normální příkazy obnovy RACF , pokud změníte, přidáte nebo odstraníte jakékoli generické profily. Například SETROPTS GENERIC (název třídy) OBNOVIT.

Pokud je však přidán, změněn nebo odstraněn profil prostředku RACF a k prostředku, pro který platí, dosud nebyl přistupováno (takže se do mezipaměti neukládají žádné informace), produkt IBM MQ použije nové informace RACF bez zadání příkazu REFRESH SECURITY.

Je-li zapnuto auditování systému RACF (například pomocí příkazu RACF RALTER AUDIT (access-pokus (audit_access_level))), nedochází k žádnému ukládání do mezipaměti, a proto IBM MQ odkazuje přímo na datový prostor RACF pro každou kontrolu. Změny jsou proto vyzvednuty okamžitě a REFRESH SECURITY není nutný pro přístup ke změnám. Můžete potvrdit, zda je auditování RACF zapnuto, pomocí příkazu RACF RLIST. Můžete například zadat příkaz

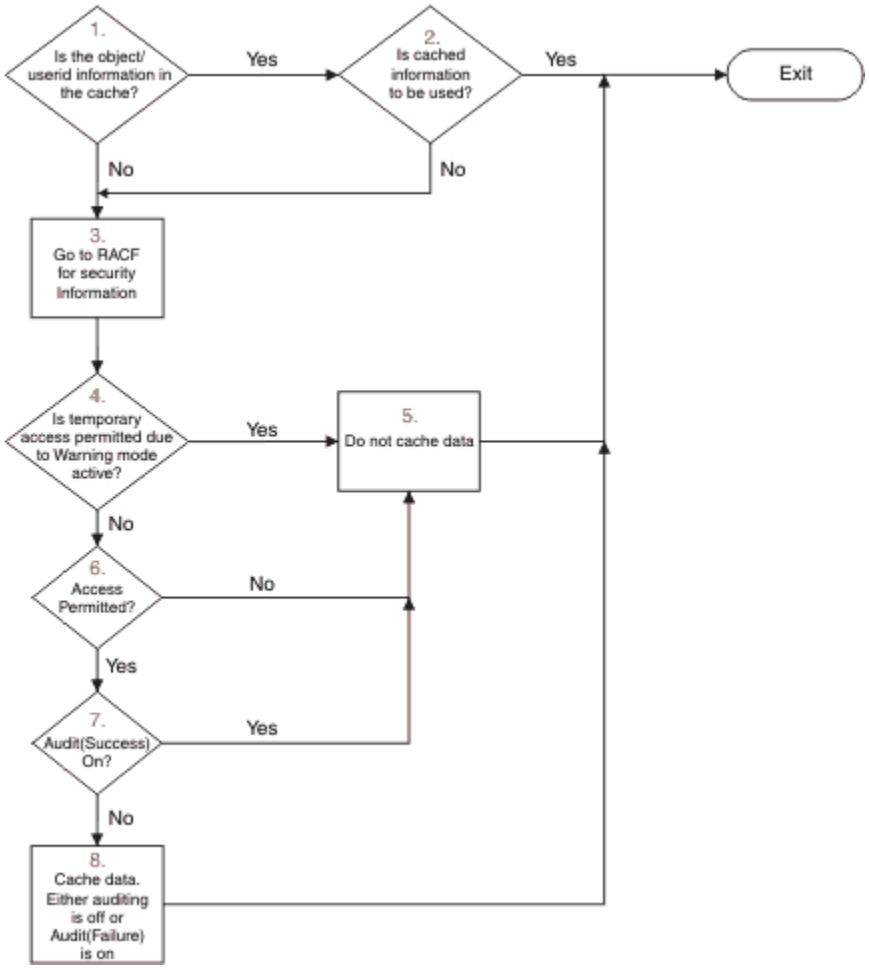
```
RLIST MQQUEUE (qmgr.SYSTEM.COMMAND.INPUT) GEN
```

a získat výsledky

```
CLASS      NAME
-----      ----
MQQUEUE    QP*.SYSTEM.COMMAND.*.** (G)
    AUDITING
    --------
    FAILURES(READ)
```

To znamená, že auditování je zapnuto. Další informace viz příručka *z/OS Security Server RACF Auditor's Guide* a *z/OS Security Server RACF Command Language Reference*.

Obrázek 17 na stránce 251 shrnuje situace, ve kterých jsou informace o zabezpečení ukládány do mezipaměti a ve kterých jsou informace ukládány do mezipaměti.



Obrázek 17. Logický tok pro ukládání do mezipaměti zabezpečení IBM MQ

Pokud změníte nastavení zabezpečení přidáním nebo odstraněním profilů přepínače ve třídách MQADMIN nebo MXADMIN, použijte jeden z těchto příkazů k dynamickému vyzvednutí těchto změn:

AKTUALIZOVAT ZABEZPEČENÍ (*)
AKTUALIZUJTE ZABEZPEČENÍ (MQADMIN)
OBNOVIT ZABEZPEČENÍ (MXADMIN)

To znamená, že můžete aktivovat nové typy zabezpečení nebo je deaktivovat bez nutnosti restartovat správce front.

Z důvodů výkonu se jedná o jediné třídy ovlivněné příkazem REFRESH SECURITY. Pokud změníte profil ve třídách MQCONN nebo MQCMDS, nemusíte používat příkaz REFRESH SECURITY.

Poznámka: Aktualizace třídy MQADMIN nebo MXADMIN není požadována, pokud změníte profil zabezpečení RESLEVEL.

Z důvodů výkonu používejte příkaz REFRESH SECURITY co nejméně často, ideálně v době mimo špičku. Počet aktualizací zabezpečení můžete minimalizovat připojením uživatelů ke skupinám RACF , které jsou již v seznamu pro přístup pro profily systému IBM MQ , spíše než umístěním jednotlivých uživatelů do seznamů pro přístup. Tímto způsobem změníte uživatele spíše než profil prostředku. Místo obnovení zabezpečení můžete také použít RVERIFY SECURITY příslušného uživatele.

Jako příklad příkazu REFRESH SECURITY předpokládejme, že definujete nové profily pro ochranu přístupu k frontám počínaje produktem INSURANCE.LIFE ve správci front PRMQ. Použijete tyto příkazy RACF :

```
RDEFINE MQQUEUE PRMQ.INSURANCE.LIFE.** UACC(NONE)
PERMIT PRMQ.INSURANCE.LIFE.** ID(LIFEGRP) ACCESS(UPDATE)
```

Musíte zadat následující příkaz, kterým sdělíte produktu RACF , aby aktualizoval informace o zabezpečení, které uchovává, například:

```
SETROPTS RACLIST(MQQUEUE) REFRESH
```

Protože jsou tyto profily generické, musíte sdělit produktu RACF , aby aktualizoval generické profily pro frontu MQQUEUE. Příklad:

```
SETROPTS GENERIC(MQQUEUE) REFRESH
```

Poté musíte pomocí tohoto příkazu sdělit správci front PRMQ, že se profily front změnily:

```
REFRESH SECURITY(MQQUEUE)
```

Aktualizace zabezpečení SSL/TLS

Chcete-li aktualizovat zobrazení úložiště klíčů TLS uložené v mezipaměti, zadejte příkaz REFRESH SECURITY s volbou TYPE (SSL). To vám umožní aktualizovat některá nastavení TLS bez nutnosti restartovat inicializátor kanálu.

z/OS *Zobrazení stavu zabezpečení*

Chcete-li zobrazit stav přepínačů zabezpečení a dalších ovládacích prvků zabezpečení, zadejte příkaz MQSC DISPLAY SECURITY.

Následující obrázek ukazuje typický výstup příkazu DISPLAY SECURITY ALL.

```
CSQH015I +CSQ1 Security timeout = 54 MINUTES
CSQH016I +CSQ1 Security interval = 12 MINUTES
CSQH030I +CSQ1 Security switches ...
CSQH034I +CSQ1 SUBSYSTEM: ON, 'SQ05.NO.SUBSYS.SECURITY' not found
CSQH032I +CSQ1 QMGR: ON, 'CSQ1.YES.QMGR.CHECKS' found
CSQH031I +CSQ1 QSG: OFF, 'SQ05.NO.QSG.CHECKS' found
CSQH031I +CSQ1 CONNECTION: OFF, 'CSQ1.NO.CONNECT.CHECKS' found
CSQH034I +CSQ1 COMMAND: ON, 'CSQ1.NO.COMMAND.CHECKS' not found
CSQH031I +CSQ1 CONTEXT: OFF, 'CSQ1.NO.CONTEXT.CHECKS' found
CSQH034I +CSQ1 ALTERNATE USER: ON, 'CSQ1.NO.ALTERNATE.USER.CHECKS' not found
CSQH034I +CSQ1 PROCESS: ON, 'CSQ1.NO.PROCESS.CHECKS' not found
CSQH034I +CSQ1 NAMELIST: ON, 'CSQ1.NO.NLIST.CHECKS' not found
CSQH034I +CSQ1 QUEUE: ON, 'CSQ1.NO.QUEUE.CHECKS' not found
CSQH034I +CSQ1 TOPIC: ON, 'CSQ1.NO.TOPIC.CHECKS' not found
CSQH031I +CSQ1 COMMAND RESOURCES: OFF, 'CSQ1.NO.CMD.RESC.CHECKS' found
CSQ9022I +CSQ1 CSQHPDTC ' DISPLAY SECURITY' NORMAL COMPLETION
```

Obrázek 18. Typický výstup z příkazu DISPLAY SECURITY

Příklad ukazuje, že správce front, který odpověděl na příkaz, má aktivní subsystém, příkaz, alternativního uživatele, proces, seznam názvů a zabezpečení fronty na úrovni správce front, ale ne na úrovni skupiny sdílení front. Připojení, prostředek příkazu a zabezpečení kontextu nejsou aktivní. Zobrazuje také, že jsou aktivní časové limity ID uživatelů a že každých 12 minut správce front kontroluje ID uživatelů, která nebyla v tomto správci front použita, a odebírá je.

Poznámka: Tento příkaz zobrazí aktuální stav zabezpečení. Nemusí nutně odrážet aktuální stav profilů přepínače definovaných pro RACFnebo stav tříd RACF . Například profily přepínače mohly být změněny od posledního restartu tohoto správce front nebo příkazu REFRESH SECURITY.

z/OS Úlohy instalace zabezpečení pro produkt z/OS

Po instalaci a přizpůsobení produktu IBM MQautorizujte procedury spuštěných úloh pro produkt RACF, autorizujte přístup k různým prostředkům a nastavte definice produktu RACF . Volitelně nakonfigurujte systém pro TLS.

Když je produkt IBM MQ poprvé nainstalován a upraven, musíte provést tyto úlohy související se zabezpečením:

1. Nastavte datovou sadu IBM MQ a zabezpečení systému pomocí:
   - Probíhá autorizace procedury started-task xxxxMSTR správce front a spuštění distribuované fronty-task procedure xxxxCHIN to run under RACF.
   - Autorizace přístupu k datovým sadám správce front.
   - Autorizace přístupu k prostředkům pro ID uživatelů, kteří budou používat správce front a obslužné programy.
   - Autorizace přístupu pro správce front, kteří budou používat struktury seznamu prostředku Coupling Facility.
   - Autorizace přístupu pro ty správce front, kteří budou používat produkt Db2.
2. Nastavte definice RACF pro zabezpečení IBM MQ .
3. Chcete-li používat protokol TLS (Transport Layer Security), připravte systém na použití certifikátů a klíčů.

z/OS *Nastavení zabezpečení datové sady IBM MQ for z/OS*

Existuje mnoho typů uživatelů IBM MQ . Pomocí funkce RACF můžete řídit jejich přístup k systémovým datovým sadám.

Mezi možné uživatele datových sad IBM MQ patří následující entity:

- Samotný správce front.
- Inicializátor kanálu

- Administrátoři produktu IBM MQ , kteří potřebují vytvořit datové sady IBM MQ , spouštět obslužné programy a podobné úlohy.
- Aplikační programátoři, kteří potřebují používat zakladače dodávané s produktem IBM MQ, zahrnují datové sady, makra a podobné prostředky.
- Žádosti, které se týkají jednoho nebo více:
  - Dávkové úlohy
  - Uživatelé TSO
  - Oblasti položek CICS
  - Oblasti položek IMS
- Datové sady CSQOUTX a CSQSNAP
- Dynamické fronty SYSTEM.CSQXCMD.*

Pro všechny tyto potenciální uživatele ochraňte datové sady IBM MQ pomocí RACF.

Musíte také řídit přístup ke všem datovým sadám 'CSQINP'.

z/OS *RACF autorizace procedur spuštěných úloh*

Některé datové sady IBM MQ jsou určeny pro výhradní použití správcem front. Pokud chráníte datové sady IBM MQ pomocí produktu RACF, musíte také autorizovat proceduru spuštěné úlohy správce front xxxxMSTRa proceduru spuštěné úlohy distribuovaného řazení do front xxxxCHINpomocí RACF. Chcete-li to provést, použijte třídu STARTED. Případně můžete použít tabulku spuštěných procedur (ICHRIN03), ale pak musíte provést IPL systému z/OS , aby se změny projevily.

Další informace viz příručka *z/OS Security Server RACF System Programmer's Guide*.

Identifikované ID uživatele RACF musí mít požadovaný přístup k datovým sadám v proceduře spuštěné úlohy. Pokud například přidružíte proceduru spuštěné úlohy správce front s názvem CSQ1MSTR k RACF ID uživatele QMGRCSQ1, musí mít ID uživatele QMGRCSQ1 přístup k prostředkům z/OS , ke kterým přistupuje správce front CSQ1 .

Také obsah pole GROUP v ID uživatele správce front musí být stejný jako obsah pole GROUP v profilu STARTED pro tohoto správce front. Pokud se obsah v každém poli GROUP neshoduje, je příslušnému ID uživatele zabráněno v vstupu do systému. Tato situace způsobí, že se produkt IBM MQ spustí s nedefinovaným ID uživatele a následně se zavře kvůli narušení zabezpečení.

ID uživatelů RACF přidružená ke spuštěným procedurám úloh správce front a inicializátoru kanálu nesmí mít nastaven atribut TRUSTED.

z/OS *Autorizace přístupu k datovým sadám*

Datové sady IBM MQ by měly být chráněny tak, aby žádný neautorizovaný uživatel nespustil instanci správce front ani nezískal přístup k žádným datům správce front. Chcete-li to provést, použijte normální ochranu datové sady produktu z/OS RACF .

Tabulka 65 na stránce 255 shrnuje RACF přístup, který musí mít spuštěná procedura úlohy správce front k různým datovým sadám.

Tabulka 65. RACF přístup k datovým sadám přidruženým ke správci front	
RACF přístup	**Datové sady**
READ (čtení)	• `thlqual.SCSQAUTH` a `thlqual.SCSQANLx` (kde x je písmeno jazyka pro váš národní jazyk). • Datové sady, na které odkazují CSQINP1, CSQINP2 a CSQXLIB v proceduře spuštěné úlohy správce front. • Datové sady SMDS vlastněné jinými správci front ve skupině. • Datové sady protokolů, BSDS a protokolů archivu pro ostatní správce front ve skupině.
AKTUALIZOVAT	• Všechny sady stránek a datové sady protokolu a BSDS. • Datové sady SMDS vlastněné správcem front • Datové sady SMDS vlastněné jinými správci front ve skupině pro struktury, které správce front provádí příkaz RECOVER CFSTRUCT.
ALTER	• Všechny datové sady protokolu archivu.

Tabulka 66 na stránce 255 shrnuje RACF přístup, který musí mít spuštěná procedura úloh pro distribuované řazení do front k různým datovým sadám.

Tabulka 66. RACF přístup k datovým sadám přidruženým k distribuovaným frontám	
RACF přístup	**Datové sady**
READ (čtení)	• thlqual.SCSQAUTH, thlqual.SCSQANLx (kde x je písmeno jazyka pro váš národní jazyk) a thlqual.SCSQMVR1. • Datové sady knihovny LE. • Datové sady, na které odkazují CSQXLIB a CSQINPX v proceduře úlohy spuštěné inicializátorem kanálu.
AKTUALIZOVAT	• Datové sady CSQOUTX a CSQSNAP

Další informace viz příručka *z/OS Security Server RACF Security Administrator's Guide*.

z/OS *Šifrování datových sad*

Datové sady IBM MQ lze šifrovat pomocí šifrování datové sady z/OS , aby byla data chráněna, nebo z regulačních důvodů.

Můžete chránit všechny sady stránek, aktivní protokol, protokol archivace a datové sady zaváděcího programu (BSDS) pomocí šifrování datové sady z/OS .

Upozornění: Sdílené datové sady zpráv (SMDS) nelze chránit pomocí šifrování datové sady z/OS pomocí produktu IBM MQ for z/OS 9.1.4 nebo dřívějšího.

Viz část důvěrnost pro data v klidu na systému IBM MQ for z/OS se šifrováním datové sady. Další informace viz.

z/OS *Nastavení zabezpečení prostředků IBM MQ for z/OS*

Existuje mnoho typů uživatelů IBM MQ . Použijte RACF k řízení jejich přístupu k prostředkům IBM MQ .

Mezi možné uživatele prostředků IBM MQ , jako jsou fronty a kanály, patří následující entity:

- Samotný správce front.
- Inicializátor kanálu

- Administrátoři produktu IBM MQ , kteří potřebují vytvářet datové sady IBM MQ , spouštět obslužné programy a podobné úlohy.
- Aplikační programátoři, kteří potřebují používat zakladače dodávané s produktem IBM MQ, zahrnují datové sady, makra a podobné prostředky.
- Žádosti, které se týkají jednoho nebo více:
  - Dávkové úlohy
  - Uživatelé TSO
  - Oblasti položek CICS
  - Oblasti položek IMS
- Datové sady CSQOUTX a CSQSNAP
- Dynamické fronty SYSTEM.CSQXCMD.*

Pro všechny tyto potenciální uživatele ochraňte prostředky IBM MQ pomocí produktu RACF. Všimněte si zejména, že iniciátor kanálu potřebuje přístup k různým prostředkům, jak je popsáno v tématu "Aspekty zabezpečení pro inicializátor kanálu v systému z/OS" na stránce 262, a proto musí být ID uživatele, pod kterým je spuštěn, autorizováno pro přístup k těmto prostředkům.

Používáte-li skupinu sdílení front, může správce front zadávat různé příkazy interně, takže ID uživatele, které používá, musí být autorizováno k zadávání těchto příkazů. Příkazy jsou:

- DEFINE, ALTER a DELETE pro každý objekt, který má QSGDISP (GROUP)
- START a STOP CHANNEL pro každý kanál používaný s CHLDISP (SHARED)

z/OS *Konfigurace systému z/OS pro použití TLS*

Toto téma použijte jako příklad konfigurace produktu IBM MQ for z/OS pomocí příkazů RACF pomocí protokolu TLS (Transport Layer Security).

Chcete-li pro zabezpečení kanálu používat protokol TLS, je třeba v systému provést řadu úloh. (Podrobnosti o použití příkazů RACF pro certifikáty a úložiště klíčů (svazky klíčů) naleznete v tématu Práce s protokolem TLS na serveru z/OS .)

1. Vytvořte svazek klíčů v produktu RACF , který bude obsahovat všechny klíče a certifikáty pro váš systém, pomocí příkazu RACF RACDCERT. Příklad:

   ```
   RACDCERT ID(CHINUSER) ADDRING(QM1RING)
   ```

   ID musí být buď ID uživatele adresního prostoru inicializátoru kanálu, nebo ID uživatele, které chcete vlastnit svazek klíčů, má-li se jednat o svazek sdílených klíčů.
2. Vytvořte digitální certifikát pro každého správce front pomocí příkazu RACF RACDCERT.

   Popisek certifikátu musí být buď hodnota atributu IBM MQ **CERTLABL** , je-li nastaven, nebo výchozí hodnota `ibmWebSphereMQ` s připojeným názvem správce front nebo skupiny sdílení front. Podrobnosti viz Popisky digitálních certifikátů . V tomto příkladu je to `ibmWebSphereMQQM1`.

   Příklad:

   ```
   RACDCERT ID(USERID) GENCERT
   SUBJECTSDN(CN('username') O('IBM') OU('departmentname') C('England'))
   WITHLABEL('ibmWebSphereMQQM1')
   ```
3. Připojte certifikát v adresáři RACF ke svazku klíčů pomocí příkazu RACF RACDCERT. Příklad:

```
RACDCERT CONNECT(ID(USERID) LABEL('ibmWebSphereMQQM1') RING(QM1RING))
CONNECT ID(CHINUSER)
```

Také musíte připojit všechny příslušné certifikáty podepsaného (od certifikační autority) ke svazku klíčů. To znamená, že všechny certifikační autority pro certifikát TLS tohoto správce front a všechny certifikační autority pro všechny certifikáty TLS, se kterými tento správce front komunikuje. Příklad:

```
RACDCERT ID(CHINUSER)
CONNECT(CERTAUTH LABEL('My CA') RING(QM1RING) USAGE(CERTAUTH))
```

4. V každém z vašich správců front zadejte pomocí příkazu IBM MQ ALTER QMGR úložiště klíčů, na které musí správce front odkazovat. Například, pokud je svazek klíčů vlastněn adresním prostorem inicializátoru kanálu:

```
ALTER QMGR SSLKEYR(QM1RING)
```

nebo pokud používáte sdílený svazek klíčů:

```
ALTER QMGR SSLKEYR(userid/QM1RING)
```

kde *userid* je ID uživatele, který vlastní sdílený svazek klíčů.

5. Seznamy odvolaných certifikátů (CRL) umožňují certifikačním autoritám odvolat certifikáty, které již nemohou být důvěryhodné. Seznamy CRL jsou uloženy na serverech LDAP. Chcete-li získat přístup k tomuto seznamu na serveru LDAP, musíte nejprve vytvořit objekt AUTHINFO s hodnotou AUTHTYPE CRLLDAP pomocí příkazu IBM MQ DEFINE AUTHINFO. Příklad:

```
DEFINE AUTHINFO(LDAP1)
AUTHTYPE(CRLLDAP)
CONNAME(ldap.server(389))
LDAPUSER('')
LDAPPWD('')
```

V tomto příkladu je seznam odvolaných certifikátů uložen ve veřejné oblasti serveru LDAP, takže pole LDAPUSER a LDAPPWD nejsou nezbytná.

Dále vložte objekt AUTHINFO do seznamu názvů pomocí příkazu IBM MQ DEFINE NAMELIST. Příklad:

```
DEFINE NAMELIST(LDAPNL) NAMES(LDAP1)
```

Nakonec přidružte seznam názvů ke každému správci front pomocí příkazu IBM MQ ALTER QMGR. Příklad:

```
ALTER QMGR SSLCRLNL(LDAPNL)
```

6. Nastavte správce front tak, aby spouštěl volání TLS, pomocí příkazu IBM MQ ALTER QMGR. To definuje dílčí úlohy serveru, které obsluhují pouze volání SSL, což ponechává normální dispečery, aby

pokračovaly ve zpracování jako normální, aniž by byly ovlivněny voláními SSL. Musíte mít alespoň dvě z těchto dílčích úloh. Příklad:

```
ALTER QMGR SSLTASKS(8)
```

Tato změna se projeví až po restartování inicializátoru kanálu.

7. Pomocí příkazu IBM MQ DEFINE CHANNEL nebo ALTER CHANNEL zadejte specifikaci šifry, která má být použita pro každý kanál. Příklad:

```
ALTER CHANNEL(LDAPCHL)
CHLTYPE(SDR)
SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA256)
```

Oba konce kanálu musí uvádět stejnou specifikaci šifry.

z/OS Správa záznamů ověřování kanálu v rámci skupiny sdílení front

Záznamy ověřování kanálu se vztahují na správce front, v němž jsou vytvořeny, a nejsou sdíleny v rámci skupiny sdílení front (QSG). Pokud jsou tedy všichni správci front ve skupině sdílení front povinni mít stejná pravidla, je třeba provést určitou správu, aby byla všechna pravidla konzistentní.

1. Vždy přidejte volbu `CMDSCOPE(*)` ke všem příkazům `SET CHLAUTH` . Tato akce odešle příkaz všem spuštěným správcům front ve skupině sdílení front.
2. Použijte příkaz `DISPLAY CHLAUTH` s volbou `CMDSCOPE(*)` a poté analyzujte odpovědi, abyste zjistili, zda jsou záznamy stejné pro všechny správce front. Když je nalezena nekonzistence, lze zadat příkaz `SET CHLAUTH` obsahující stejné pravidlo s `CMDSCOPE(*)` nebo `CMDSCOPE(`*qmgr-name*`)`.
3. Přidejte člena do zřetězení CSQINP2 správce front (podrobnosti viz Příkazy inicializace), který má úplnou sadu pravidel. Tyto informace budou načteny jako součást procesu inicializace správce front. Pokud příkaz `SET CHLAUTH` používá `ACTION(ADD)` , pravidlo se přidá pouze v případě, že neexistovalo. Použití `ACTION(REPLACE)` nahradí existující pravidlo, pokud již existuje, nebo jej přidá, pokud neexistuje. Téhož člena lze poté umístit do zřetězení CSQINP2 všech správců front ve skupině sdílení front.
4. Pomocí obslužného programu CSQUTIL (podrobnosti naleznete v tématu Vydávání příkazů do adresáře IBM MQ (COMMAND)) extrahujte pravidla z jednoho správce front pomocí volby `MAKEDEF` nebo `MAKEREP` . Poté přehrajte výstup pomocí CSQUTIL do cílového správce front.

Související pojmy

Záznamy ověření kanálu

Chcete-li zlepšit kontrolu nad udílením přístupu k připojujícím se systémům na úrovni kanálu, můžete použít záznamy ověření kanálu.

z/OS Aspekty auditování v systému z/OS

Pro provádění auditu zabezpečení správce front jsou k dispozici běžné ovládací prvky auditování systému RACF . Produkt IBM MQ neshromažďuje žádné vlastní statistiky zabezpečení. Jediné statistiky jsou ty, které lze vytvořit auditováním.

Auditování RACF může být založeno na:

- ID uživatelů
- Třídy prostředků
- Profily

Další podrobnosti viz příručka *z/OS Security Server RACF Auditor's Guide*.

Poznámka: Auditování snižuje výkon; čím více auditování implementujete, tím více výkonu snížíte. Toto je také zvážení použití volby RACF VAROVÁNÍ.

z/OS *Auditování RESLEVEL*

Systémový parametr RESAUDIT použijte k řízení produkce záznamů auditu RESLEVEL. RACF Jsou vytvářeny obecné záznamy auditu.

Vytvářejte záznamy auditu RESLEVEL nastavením parametru systému RESAUDIT na hodnotu YES. Je-li parametr RESAUDIT nastaven na hodnotu NO, záznamy auditu se nevytvoří. Další podrobnosti o nastavení tohoto parametru viz Použití CSQ6SYSP.

Je-li volba RESAUDIT nastavena na hodnotu YES, nejsou při kontrole RESLEVEL provedeny žádné normální záznamy auditu RACF , aby se zjistilo, jaký přístup má ID uživatele adresního prostoru k profilu hlq.RESLEVEL . Místo toho IBM MQ požaduje, aby RACF vytvořil OBECNÝ záznam auditu (událost číslo 27). Tyto kontroly se provádějí pouze v době připojení, takže náklady na výkon jsou minimální.

Upozornění: RACFRW již není navrhovaným obslužným programem pro zpracování záznamů auditu RACF . Měli byste použít RACF obslužný program pro uvolnění dat SMF , protože se jedná o upřednostňovanou metodu vytváření sestav.

Obecné záznamy auditu IBM MQ můžete hlásit pomocí RACFRW (RACF report writer). K ohlášení přístupu RESLEVEL můžete použít následující příkazy RACFRW:

```
RACFRW
SELECT PROCESS
EVENT GENERAL
LIST
END
```

Ukázková sestava z RACFRW, s výjimkou polí *Date*, *Time*a *SYSID* , je zobrazena v souboru Obrázek 19 na stránce 259.

```
       RACF REPORT - LISTING OF PROCESS RECORDS                                  PAGE   4
                                E
                                V  Q
                                E  U
*JOB/USER *STEP/  --TERMINAL--  N  A
   NAME    GROUP     ID    LVL  T  L

 WS21B    MQMGRP IGJZM000   0   27 0  JOBID=(WS21B 05.111 09:44:57),USERDATA=()
    TRUSTED USER                      AUTH=(NONE),REASON=(NONE)
                                SESSION=TSOLOGON,TERMINAL=IGJZM000,
                                LOGSTR='CSQH RESLEVEL CHECK PERFORMED AGAINST
PROFILE(QM66.RESLEVEL),
                                CLASS(MQADMIN), ACCESS EQUATES TO
(CONTROL)',RESULT=SUCCESS,MQADMIN
```

Obrázek 19. Ukázkový výstup z RACFRW zobrazující obecné záznamy auditu RESLEVEL

Při kontrole dat LOGSTR v tomto ukázkovém výstupu můžete vidět, že uživatel TSO WS21B má přístup CONTROL k souboru QM66.RESLEVEL. To znamená, že všechny kontroly zabezpečení prostředků jsou vynechány, když uživatel WS21B přistupuje k prostředkům QM66 .

Další informace o použití RACFRW viz Zapisovač sestav RACF v příručce *z/OS Security Server RACF Auditor's Guide*.

z/OS Přizpůsobení zabezpečení

Chcete-li změnit způsob fungování zabezpečení systému IBM MQ , musíte tak učinit prostřednictvím uživatelské procedury SAF (ICHRFR00) nebo prostřednictvím ukončení v externím správci zabezpečení.

Další informace o uživatelských procedur systému RACF naleznete v dokumentaci *z/OS Odkaz na makro RACROUTE serveru zabezpečení* .

Poznámka: Protože produkt IBM MQ optimalizuje volání do ESM, požadavky RACROUTE nemusí být provedeny například na každém otevření pro konkrétní frontu konkrétním uživatelem.

z/OS Zprávy narušení zabezpečení na systému z/OS

Narušení zabezpečení je označeno návratovým kódem MQRC_NOT_AUTHORIZED v aplikačním programu nebo zprávou v protokolu úlohy.

Návratový kód MQRC_NOT_AUTHORIZED lze vrátit do aplikačního programu z následujících důvodů:

- Uživateli není povoleno připojit se ke správci front. V tomto případě obdržíte zprávu ICH408I v protokolu úloh Batch/TSO, CICSnebo IMS .
- Přihlášení uživatele ke správci front se nezdařilo, protože například ID uživatele úlohy je neplatné nebo vhodné, nebo ID uživatele úlohy nebo alternativní ID uživatele je neplatné. Jedno nebo více těchto ID uživatelů nemusí být platných, protože byla zrušena nebo odstraněna. V tomto případě obdržíte zprávu ICHxxxx a možná i zprávu IRRxxxx v protokolu úlohy správce front s uvedením příčiny selhání přihlášení. Příklad:

```
ICH408I USER(NOTDFND ) GROUP(        ) NAME(???                 )
  LOGON/JOB INITIATION - USER AT TERMINAL          NOT RACF-DEFINED
IRR012I  VERIFICATION FAILED. USER PROFILE NOT FOUND
```

- Byl požadován alternativní uživatel, ale ID uživatele úlohy nemá přístup k alternativnímu ID uživatele. V případě tohoto selhání se v protokolu úloh příslušného správce front zobrazí zpráva o narušení.
- Volba kontextu byla použita nebo je odvozena otevřením přenosové fronty pro výstup, ale ID uživatele úlohy nebo, kde je to možné, ID úlohy nebo alternativního uživatele nemá přístup k volbě kontextu. V tomto případě je do protokolu úloh příslušného správce front vložena zpráva o narušení.
- Neautorizovaný uživatel se pokusil o přístup k zabezpečenému objektu správce front, například k frontě. V tomto případě se zpráva ICH408I pro narušení vloží do protokolu úlohy příslušného správce front. Toto narušení může být způsobeno úlohou nebo, je-li to vhodné, úlohou nebo alternativním ID uživatele.

Zprávy o narušení zabezpečení příkazů a zabezpečení prostředků příkazů lze nalézt také v protokolu úloh správce front.

Pokud zpráva o narušení ICH408I zobrazuje název úlohy správce front spíše než ID uživatele, jedná se obvykle o výsledek zadání prázdného alternativního ID uživatele. Příklad:

```
ICH408I JOB(MQS1MSTR) STEP(MQS1MSTR)
          MQS1.PAYROLL.REQUEST CL(MQQUEUE)
          INSUFFICIENT ACCESS AUTHORITY
          ACCESS INTENT(UPDATE )  ACCESS ALLOWED(NONE   )
```

Můžete zjistit, kdo může používat prázdná alternativní ID uživatelů, kontrolou seznamu pro přístup profilu MQADMIN hlq.ALTERNATE.USER.-BLANK-.

Zprávu o narušení ICH408I může generovat také:

- Příkaz odesílaný do vstupní fronty systémového příkazu bez kontextu. Programy napsané uživatelem, které zapisují do vstupní fronty systémového příkazu, by měly vždy používat kontextovou volbu. Další informace viz téma “Profily pro zabezpečení kontextu” na stránce 217.
- Když úloha přistupující k prostředku IBM MQ nemá přidružené ID uživatele, nebo když adaptér IBM MQ nemůže extrahovat ID uživatele z prostředí adaptéru.

Zprávy o narušení mohou být také vydány, pokud používáte jak skupinu sdílení front, tak zabezpečení na úrovni správce front. Mohou se zobrazit zprávy informující o tom, že na úrovni správce front nebyl nalezen žádný profil, ale přesto mu byl udělen přístup kvůli profilu na úrovni skupiny sdílení front.

```
ICH408I JOB(MQS1MSTR) STEP(MQS1MSTR)
          MQS1.PAYROLL.REQUEST CL(MQQUEUE)
          PROFILE NOT FOUND - REQUIRED FOR AUTHORITY CHECKING
          ACCESS INTENT(UPDATE )  ACCESS ALLOWED(NONE   )
```

Další informace o zprávách ICH408I naleznete v dokumentaci k produktu z/OS for Security Server RACF Messages and Codes .

z/OS Co dělat, když je přístup povolen nebo zakázán nesprávně

Kromě informací uvedených v dokumentaci k produktu z/OS použijte tento kontrolní seznam, pokud se zdá, že přístup k prostředku je nesprávně řízen.

Podrobné kroky, pokud je přístup povolen nebo zakázán, naleznete v příručce *z/OS Security Server RACF Security Administrator's Guide* .

- Jsou profily přepínače správně nastaveny?
  - Je RACF aktivní?
  - Jsou třídy produktu IBM MQ RACF nainstalovány a aktivní?

    Použijte příkaz RACF , SETROPTS LIST, abyste to zkontrolovali.
  - Pomocí příkazu IBM MQ DISPLAY SECURITY můžete zobrazit aktuální stav přepínače ze správce front.
  - Zkontrolujte profily přepínače ve třídě MQADMIN.

    K tomu použijte příkazy RACF , SEARCH a RLIST.
  - Znovu zkontrolujte profily přepínače RACF zadáním příkazu IBM MQ REFRESH SECURITY (MQADMIN).
- Změnil se profil prostředku RACF ? Došlo například ke změně univerzálního přístupu k profilu nebo ke změně seznamu pro přístup k profilu?
  - Je profil generický?

    Pokud ano, zadejte příkaz RACF , SETROPTS GENERIC (název třídy) OBNOVIT.
  - Aktualizovali jste zabezpečení tohoto správce front?

    V případě potřeby zadejte příkaz RACF SETROPTS RACLIST (classname) OBNOVIT.

    V případě potřeby zadejte příkaz IBM MQ REFRESH SECURITY (*).
- Změnila se definice uživatele RACF ? Například, byl uživatel připojen k nové skupině, nebo bylo přístupové oprávnění uživatele odvoláno?
  - Ověřili jste uživatele zadáním příkazu IBM MQ RVERIFY SECURITY (userid)?
- Jsou kontroly zabezpečení vynechány kvůli RESLEVEL?
  - Zkontrolujte přístup připojujícího se ID uživatele k profilu RESLEVEL. Pomocí záznamů auditu RACF určete, na co je nastaven parametr RESLEVEL.
  - U kanálů nezapomeňte, že úroveň přístupu, kterou má ID uživatele inicializátoru kanálu na hodnotu RESLEVEL, je zděděna všemi kanály, takže úroveň přístupu, například ALTER, která způsobí vynechání všech kontrol, způsobí vynechání kontrol zabezpečení pro všechny kanály.
  - Pokud spouštíte produkt CICS, zkontrolujte nastavení RESSEC transakce.
  - Pokud byl parametr RESLEVEL změněn v době, kdy je uživatel připojen, musí se odpojit a znovu připojit, aby se nové nastavení RESLEVEL projevilo.
- Používáte skupiny sdílení front?

- Používáte-li skupinu sdílení front i zabezpečení na úrovni správce front, zkontrolujte, zda jste definovali všechny správné profily. Není-li profil správce front definován, odešle se do protokolu zpráva, že profil nebyl nalezen.
- Použili jste kombinaci nastavení přepínače, která nejsou platná, takže byla nastavena úplná kontrola zabezpečení?
- Potřebujete definovat přepínače zabezpečení pro přepsání některých nastavení skupiny sdílení front pro vašeho správce front?
- Má profil na úrovni správce front přednost před profilem na úrovni skupiny sdílení front?

z/OS Aspekty zabezpečení pro inicializátor kanálu v systému z/OS

Používáte-li zabezpečení prostředků v prostředí distribuovaných front, potřebuje adresní prostor inicializátoru kanálu odpovídající přístup k různým prostředkům produktu IBM MQ . K zavedení algoritmu ochrany hesla můžete použít zařízení ICSF (Integrated Cryptographic Support Facility).

Další informace o ICSF naleznete v dokumentaci k produktu z/OS Cryptographic Services .

Použití zabezpečení prostředků

Pokud používáte zabezpečení prostředků, zvažte následující body, pokud používáte distribuované řazení do front:

systémových front
Adresní prostor inicializátoru kanálu vyžaduje přístup příkazu RACF UPDATE k systémovým frontám uvedeným v seznamu “Zabezpečení systémové fronty” na stránce 206a ke všem cílovým frontám uživatele a frontě nedoručených zpráv (viz “Zabezpečení fronty nedoručených zpráv” na stránce 205).

Přenosové fronty
Adresní prostor inicializátoru kanálu vyžaduje přístup ALTER ke všem uživatelským přenosovým frontám.

zabezpečení kontextu
ID uživatele kanálu (a ID uživatele MCA, pokud bylo určeno) potřebují přístup RACF CONTROL k profilům hlq.CONTEXT.queuename ve třídě MQADMIN. V závislosti na profilu RESLEVEL může ID uživatele kanálu také vyžadovat přístup CONTROL k těmto profilům.

Všechny kanály potřebují přístup CONTROL k MQADMIN hlq.CONTEXT. profil fronty nedoručených zpráv. Všechny kanály (ať už zahajují nebo odpovídají) mohou generovat sestavy, a proto potřebují přístup CONTROL k profilu hlq.CONTEXT.reply-q .

Kanály SENDER, CLUSSDR a SERVER potřebují přístup CONTROL k profilům hlq.CONTEXT.xmit-queue-name , protože zprávy lze vložit do přenosové fronty, aby se kanál probudil a postupně ukončil.

Poznámka: Pokud má ID uživatele kanálu nebo skupina RACF , ke které je ID uživatele kanálu připojeno, přístup CONTROL nebo ALTER k příkazu hlq.RESLEVEL, nejsou pro inicializátor kanálu ani žádný z jeho kanálů prováděny žádné kontroly prostředků.

Další informace viz “Profily pro zabezpečení kontextu” na stránce 217 “RESLEVEL a připojení inicializátoru kanálu” na stránce 237 a “ID uživatelů pro kontrolu zabezpečení na systému z/OS” na stránce 239 .

CSQINPX
Pokud používáte vstupní datovou sadu CSQINPX, iniciátor kanálu také potřebuje přístup READ k CSQINPX a přístup UPDATE k datové sadě CSQOUTX a dynamickým frontám SYSTEM.CSQXCMD.*.

Zabezpečení připojení
Požadavky na připojení adresního prostoru inicializátoru kanálu používají typ připojení CHIN, pro který musí být nastaveno odpovídající zabezpečení přístupu, viz “Profily zabezpečení připojení pro inicializátor kanálu” na stránce 200.

Datové sady
Adresní prostor inicializátoru kanálu vyžaduje odpovídající přístup k datovým sadám správce front. Viz téma “Autorizace přístupu k datovým sadám” na stránce 254.

Příkazy
Distribuované příkazy řazení do front (například DEFINE CHANNEL, START CHINIT, START LISTENER a další příkazy kanálu) musí mít nastaveno odpovídající zabezpečení příkazů, viz Tabulka 49 na stránce 220.

Používáte-li skupinu sdílení front, iniciátor kanálu může interně zadat různé příkazy, takže ID uživatele, které používá, musí být autorizováno k zadávání těchto příkazů. Tyto příkazy jsou START a STOP CHANNEL pro každý kanál používaný s CHLDISP (SHARED).

Pokud režim PSMODE správce front není DISABLED, musí mít inicializátor kanálu přístup READ k příkazu DISPLAY PUBSUB.

Zabezpečení kanálu
Kanály, zejména přijímače a připojení serverů, vyžadují nastavení příslušného zabezpečení. Další informace naleznete v části “ID uživatelů pro kontrolu zabezpečení na systému z/OS” na stránce 239 .

K zajištění zabezpečení kanálů můžete také použít protokol TLS (Transport Layer Security). Další informace o použití protokolu TLS s produktem IBM MQnaleznete v tématu “Protokoly zabezpečení TLS v adresáři IBM MQ” na stránce 24 .

Informace o zabezpečení připojení serveru viz také “Řízení přístupu pro klienty” na stránce 102 .

ID uživatelů
ID uživatelů popsaná v části “ID uživatelů používaná inicializátorem kanálu” na stránce 242 a “ID uživatelů používaná agentem front v rámci skupiny” na stránce 246 vyžadují následující přístup:

- RACF UPDATE přístup k příslušným cílovým frontám a frontě nedoručených zpráv
- RACF Přístup CONTROL k profilu `hlq.CONTEXT.queuename` , pokud je kontrola kontextu prováděna na přijímači
- Odpovídající přístup k souboru hlq.ALTERNATE.USER.userid mohou vyžadovat použití.
- Pro klienty odpovídající přístup RACF k prostředkům, které se mají použít.

Zabezpečení APPC
Nastavte odpovídající zabezpečení APPC, pokud používáte přenosový protokol LU 6.2 . (Použijte například třídu APPCLU RACF .) Informace o nastavení zabezpečení pro APPC naleznete v následující dokumentaci:

- *z/OS MVS Plánování: Správa APPC*
- *z/OS MVS Programování: Zápis serverů pro APPC/MVS*

Odchozí přenosy používají volbu "SECURITY (SAME)" APPC. Výsledkem je, že ID uživatele adresního prostoru inicializátoru kanálu a jeho výchozí profil (RACF GROUP) jsou v síti protékány k přijímači s indikátorem, že ID uživatele již bylo ověřeno (ALREADYV).

Pokud je přijímající strana také z/OS, ID uživatele a profil jsou ověřeny APPC a ID uživatele je prezentováno kanálu příjemce a použito jako ID uživatele kanálu.

V prostředí, ve kterém správce front používá APPC ke komunikaci s jiným správcem front ve stejném nebo jiném systému z/OS , je třeba zajistit, aby:

- Definice VTAM pro komunikující LU určuje SETACPT (ALREADYV)
- Existuje profil RACF APPCLU pro připojení mezi LU, který uvádí CONVSEC (ALREADYV)

Změna nastavení zabezpečení
Pokud se změní úroveň přístupu RACF , kterou má ID uživatele kanálu nebo ID uživatele MCA k cílové frontě, projeví se tato změna pouze pro nové obslužné rutiny objektů (tj. nové `MQOPEN`) pro cílovou frontu. Časy, kdy jsou otevřené a zavřené fronty MCA proměnlivé. Pokud je kanál již spuštěn při změně přístupu, může MCA nadále vkládat zprávy do cílové fronty s použitím stávajícího zabezpečeného

přístupu ID uživatelů, a nikoli aktualizovaného zabezpečeného přístupu. Zastavení a restartování kanálů pro vynucení aktualizované úrovně přístupu se tomuto scénáři vyhýbá.

automatický restart
Používáte-li k restartování inicializátoru kanálu správce ARM (Automatic Restart Manager) systému z/OS , musí být ID uživatele přidružené k adresnímu prostoru XCFAS autorizováno k zadání příkazu IBM MQ START CHINIT.

Použití ICSF (Integrated Cryptographic Service Facility)

Inicializátor kanálu může použít ICSF ke generování náhodného čísla při zavedení algoritmu ochrany hesla pro zamlžení hesel proudících přes kanály klienta, pokud není použito TLS. Proces generování náhodného čísla se nazývá *entropie*.

Máte-li nainstalovanou funkci z/OS , ale nespustili jste ICSF, zobrazí se zpráva CSQX213E a inicializátor kanálu používá STCK pro entropii.

Zpráva CSQX213E vás varuje, že algoritmus ochrany hesla není tak zabezpečený, jak by mohl být. Můžete však pokračovat ve svém procesu; na běhové prostředí to nemá žádný další dopad.

Pokud nemáte nainstalovanou funkci z/OS , iniciátor kanálu automaticky použije STCK.

Notes:

1. Použití ICSF pro entropii generuje více náhodných sekvencí než použití STCK.
2. Pokud spustíte ICSF, musíte restartovat inicializátor kanálu.
3. ICSF je vyžadováno pro určité CipherSpecs. Pokud se pokusíte použít jednu z těchto CipherSpecs a nemáte nainstalovanou komponentu ICSF, obdržíte zprávu CSQX629E.

z/OS Zabezpečení v klastrech správců front v systému z/OS

Aspekty zabezpečení pro klastry jsou stejné pro správce front a kanály, které nejsou klastrované. Inicializátor kanálu potřebuje přístup k některým dalším systémovým frontám a některé další příkazy vyžadují odpovídající sadu zabezpečení.

K ověřování kanálů klastru můžete použít ID uživatele MCA, záznamy ověřování kanálu, protokol TLS a uživatelské procedury zabezpečení (stejně jako u konvenčních kanálů). Záznamy ověřování kanálu nebo uživatelská procedura zabezpečení týkající se přijímacího kanálu klastru musí zkontrolovat, zda má vzdálený správce front povolen přístup k frontám klastru správce front serveru. Můžete začít používat podporu klastru IBM MQ , aniž byste změnili existující zabezpečení přístupu k frontě. Ostatním správcům front v klastru však musíte povolit zápis do systému SYSTEM.CLUSTER.COMMAND.QUEUE , pokud se mají připojit ke klastru.

Podpora klastru IBM MQ neposkytuje mechanizmus pro omezení člena klastru pouze na roli klienta. V důsledku toho se musíte ujistit, že důvěřujete všem správcům front, které povolíte do klastru. Pokud některý správce front v klastru vytvoří frontu s konkrétním názvem, může pro tuto frontu přijímat zprávy bez ohledu na to, zda aplikace vkládala zprávy do této fronty, či nikoli.

Chcete-li omezit členství v klastru, proveďte stejnou akci, kterou byste měli provést, abyste zabránili připojení správců front k přijímacím kanálům. Členství v klastru můžete omezit pomocí záznamů ověřování kanálu nebo napsáním programu uživatelské procedury zabezpečení v přijímacím kanálu. Můžete také napsat uživatelský program, který zabrání neoprávněným správcům front v zápisu do systému SYSTEM.CLUSTER.COMMAND.QUEUE.

Poznámka: Není vhodné povolit aplikacím otevření systému SYSTEM.CLUSTER.TRANSMIT.QUEUE přímo. Také není vhodné povolit, aby aplikace přímo otevřela jakoukoli jinou přenosovou frontu.

Pokud používáte zabezpečení prostředků, zvažte kromě aspektů uvedených v části “Aspekty zabezpečení pro inicializátor kanálu v systému z/OS” na stránce 262také následující body:

systémových front
Inicializátor kanálu potřebuje přístup pomocí příkazu RACF ALTER k následujícím systémovým frontám:

- SYSTEM.CLUSTER.COMMAND FRONTA
- SYSTEM.CLUSTER.TRANSMIT.QUEUE.

a přístup UPDATE k SYSTEM.CLUSTER.REPOSITORY.QUEUE

Také potřebuje přístup READ ke všem seznamům názvů používaným pro klastrování.

Příkazy
Nastavte odpovídající zabezpečení příkazu (jak je popsáno v tématu Tabulka 49 na stránce 220). pro příkazy podpory klastrů (REFRESH a RESET CLUSTER, SUSPEND a RESUME QMGR.

z/OS Aspekty zabezpečení pro použití IBM MQ s CICS

Všechny verze produktu CICS podporované produktem IBM MQ 9.0.0a novější používají verzi adaptéru a mostu dodanou s produktem CICS .

Podrobnosti o aspektech zabezpečení viz:

- Zabezpečení pro adaptér CICS-MQ.
- Zabezpečení pro most CICS-MQ.

z/OS Aspekty zabezpečení pro použití IBM MQ s IMS

Toto téma použijte k plánování požadavků na zabezpečení, když používáte produkt IBM MQ s produktem IMS.

Použití třídy OPERCMDS

Používáte-li produkt RACF k ochraně prostředků ve třídě OPERCMDS, ujistěte se, že ID uživatele přidružené k adresnímu prostoru správce front IBM MQ má oprávnění k zadání příkazu MODIFY pro libovolný systém IMS , ke kterému se může připojit.

Aspekty zabezpečení pro most IMS

Při rozhodování o požadavcích na zabezpečení pro most IMS je třeba vzít v úvahu čtyři aspekty:

- Jaká bezpečnostní autorizace je potřebná pro připojení IBM MQ k IMS
- Kolik kontrol zabezpečení se provádí na aplikacích používajících most pro přístup k produktu IMS
- Které prostředky IMS mohou tyto aplikace používat
- Jaká autorita má být použita pro zprávy, které jsou vloženy a přijaty mostem

Když definujete požadavky na zabezpečení pro most IMS , musíte zvážit následující:

- Zprávy procházející přes most mohou pocházet z aplikací na platformách, které nenabízejí silné funkce zabezpečení.
- Zprávy procházející přes most mohly pocházet z aplikací, které nejsou řízeny stejným podnikem nebo organizací.

z/OS *Aspekty zabezpečení pro připojení k produktu IMS*

Udělte ID uživatele adresního prostoru správce front IBM MQ přístup ke skupině OTMA.

Most IMS je klientem OTMA. Připojení k produktu IMS pracuje pod ID uživatele adresního prostoru správce front IBM MQ . Tato volba je obvykle definována jako člen spuštěné skupiny úloh. Tomuto ID uživatele musí být udělen přístup ke skupině OTMA (pokud není nastavení /SECURE OTMA NONE).

Chcete-li to provést, definujte následující profil ve třídě FACILITY:

```
IMSXCF.xcfgname.mqxcfmname
```

Kde `xcfgname` je název skupiny XCF a `mqxcfmname` je název člena XCF IBM MQ.

K tomuto profilu je třeba udělit ID uživatele správce front IBM MQ přístup pro čtení.

Poznámka:

1. Změníte-li oprávnění ve třídě FACILITY, musíte zadat příkaz RACF SETROPTS RACLIST (FACILITY) REFRESH, aby se změny aktivovaly.
2. Pokud profil hlq.NO.SUBSYS.SECURITY existuje ve třídě MQADMIN, nepředá se IMS žádné ID uživatele a připojení se nezdaří, pokud není nastavení /SECURE OTMA NONE.

z/OS *Řízení přístupu k aplikaci pro most IMS*

Definujte profil RACF ve třídě FACILITY pro každý systém IMS . Udělte odpovídající úroveň přístupu k ID uživatele správce front IBM MQ .

Pro každý systém IMS , ke kterému se připojuje most IMS , můžete definovat následující profil RACF ve třídě FACILITY, abyste určili, kolik kontroly zabezpečení se provede pro každou zprávu předanou systému IMS .

```
IMSXCF.xcfgname.imsxcfmname
```

Kde `xcfgname` je název skupiny XCF a `imsxcfmname` je název člena XCF pro IMS. (Musíte definovat samostatný profil pro každý systém IMS .)

Úroveň přístupu, kterou povolíte pro ID uživatele správce front IBM MQ v tomto profilu, je vrácena produktu IBM MQ při připojení mostu IMS k produktu IMSa označuje úroveň zabezpečení, která je vyžadována pro následné transakce. Pro následné transakce produkt IBM MQ požaduje odpovídající služby z produktu RACF , a kde je ID uživatele autorizováno, předá zprávu do produktu IMS.

OTMA nepodporuje příkaz IMS /SIGN; avšak IBM MQ vám umožňuje nastavit kontrolu přístupu pro každou zprávu, abyste umožnili implementaci nezbytné úrovně řízení.

Mohou být vráceny následující informace o úrovni přístupu:

NEBYL NALEZEN ŽÁDNÝ PROFIL
: Tyto hodnoty označují, že je vyžadováno maximální zabezpečení, to znamená, že pro každou transakci je vyžadováno ověření. Provede se kontrola, zda je ID uživatele zadané v poli *UserIdentifier* struktury MQMD a heslo nebo PassTicket v poli *Authenticator* struktury MQIIH známé produktu RACFa jedná se o platnou kombinaci. Vytvoří se UTOKEN s heslem nebo PassTicketa předá se IMS ; UTOKEN není uložen do mezipaměti.

  Poznámka: Pokud profil hlq.NO.SUBSYS.SECURITY existuje ve třídě MQADMIN, tato úroveň zabezpečení přepíše to, co je definováno v profilu.

READ (čtení)
: Tato hodnota označuje, že se má provést stejné ověření jako pro `NONE` za následujících okolností:

  - Při prvním zjištění specifického ID uživatele
  - Když bylo ID uživatele zjištěno dříve, ale UTOKEN uložený v mezipaměti nebyl vytvořen s heslem nebo PassTicket

  IBM MQ si vyžádá UTOKEN, je-li požadován, a předá jej do IMS.

  Poznámka: Pokud byl požadavek na opětovné ověření zabezpečení zpracován, všechny informace uložené v mezipaměti jsou ztraceny a při prvním zjištění každého ID uživatele je požadován UTOKEN.

AKTUALIZOVAT
: Provede se kontrola, zda je ID uživatele v poli *UserIdentifier* struktury MQMD známé produktu RACF.

  UTOKEN je sestaven a předán do adresáře IMS ; UTOKEN je uložen do mezipaměti.

OVLÁDÁNÍ/ZMĚNA
Tyto hodnoty označují, že pro žádná ID uživatelů pro tento systém IMS není třeba zadávat žádné bezpečnostní klíče UTOKENs. (Tuto volbu byste pravděpodobně použili pouze pro vývojové a testovací systémy.)

Upozornění: Všimněte si, že ID uživatele obsažené v poli *UserIdentifier* struktury MQMD je stále předáno pro **CONTROL/ALTER**.

Poznámka:

1. Tento přístup je definován, když se IBM MQ připojuje k IMSa trvá po dobu trvání připojení. Chcete-li změnit úroveň zabezpečení, je třeba změnit přístup k profilu zabezpečení a poté most zastavit a restartovat (například zastavením a restartováním OTMA).
2. Změníte-li oprávnění ve třídě FACILITY, musíte zadat příkaz RACF SETROPTS RACLIST (FACILITY) REFRESH, aby se změny aktivovaly.
3. Můžete použít heslo nebo PassTicket, ale musíte si uvědomit, že most IMS nešifruje data. Chcete-li získat informace o použití PassTickets, prohlédněte si téma "Použití RACF PassTickets v záhlaví IMS" na stránce 268.
4. Některé z těchto výsledků mohou být ovlivněny nastavením zabezpečení v souboru IMSpomocí příkazu /SECURE OTMA.
5. Informace UTOKEN uložené v mezipaměti jsou uchovávány po dobu trvání definovanou parametry INTERVAL a TIMEOUT příkazu IBM MQ ALTER SECURITY.
6. Volba RACF WARNING nemá žádný vliv na profil IMSXCF.xcfgname.imsxcfmname . Jeho použití nemá vliv na úroveň uděleného přístupu a nejsou vytvářeny žádné zprávy RACF VAROVÁNÍ.

z/OS *Kontrola zabezpečení na systému IMS*

Zprávy, které procházejí přes most, obsahují informace o zabezpečení. Provedené kontroly zabezpečení závisí na nastavení příkazu IMS /SECURE OTMA.

Každá zpráva produktu IBM MQ , která prochází přes most, obsahuje následující informace o zabezpečení:

- ID uživatele obsažené v poli *UserIdentifier* struktury MQMD
- Obor zabezpečení obsažený v poli *SecurityScope* struktury MQIIH (je-li přítomna struktura MQIIH).
- UTOKEN (pokud podsystém IBM MQ nemá přístup CONTROL nebo ALTER k příslušnému profilu `IMSXCF.xcfgname.imsxcfmname`)

Provedené kontroly zabezpečení závisí na nastavení příkazu IMS /SECURE OTMA, jak je uvedeno níže:

/ZABEZPEČENÁ ŽÁDNÁ OTMA
Pro transakci se neprovádějí žádné kontroly zabezpečení.

/BEZPEČNÁ KONTROLA OTMA
Pole *UserIdentifier* struktury MQMD je předáno produktu IMS pro kontrolu oprávnění transakcí nebo příkazů.

V řídicí oblasti IMS je sestaven prvek ACEE (Accessor Environment Element).

/BEZPEČNÉ ZAPLNĚNÍ OTMA
Pole *UserIdentifier* struktury MQMD je předáno produktu IMS pro kontrolu oprávnění transakcí nebo příkazů.

Prostředí ACEE je sestaveno v závislé oblasti IMS a v řídicí oblasti IMS .

/ZABEZPEČENÝ PROFIL OTMA
Pole *UserIdentifier* struktury MQMD je předáno produktu IMS pro kontrolu oprávnění transakcí nebo příkazů.

Pole *SecurityScope* ve struktuře MQIIH se používá k určení, zda se má sestavit ACEE v závislé oblasti IMS a řídicí oblasti.

Poznámka:

1. Pokud změníte oprávnění ve třídě TIMS nebo CIMS nebo v přidružených třídách skupiny GIMS nebo DIMS, musíte k aktivaci změn zadat následující příkazy IMS :
   - /UPRAVIT PŘÍPRAVU RACF
   - /UPRAVIT POTVRZENÍ
2. Pokud nepoužijete /SECURE OTMA PROFILE, bude jakákoli hodnota uvedená v poli **SecurityScope** struktury MQIIH ignorována.

z/OS *Kontrola zabezpečení prováděnou mostem IMS*

V závislosti na prováděné akci se používají různá oprávnění.

Když most vloží nebo obdrží zprávu, použijí se následující oprávnění:

Získání zprávy z fronty mostu
Neprovádějí se žádné kontroly zabezpečení.

Vložení výjimky nebo zprávy sestavy COA
Používá oprávnění ID uživatele v poli *UserIdentifier* struktury MQMD.

Vložení zprávy s odpovědí
Používá oprávnění ID uživatele v poli *UserIdentifier* struktury MQMD původní zprávy.

Vložení zprávy do fronty nedoručených zpráv
Neprovádějí se žádné kontroly zabezpečení.

Poznámka:

1. Pokud změníte profily tříd IBM MQ , musíte k aktivaci změn zadat příkaz IBM MQ REFRESH SECURITY (*).
2. Změníte-li oprávnění uživatele, musíte k aktivaci změny zadat příkaz MQSC RVERIFY SECURITY.

z/OS *Použití RACF PassTickets v záhlaví IMS*

Místo hesla v záhlaví IMS můžete použít PassTicket .

Chcete-li použít PassTicket místo hesla v záhlaví IMS (MQIIH), uveďte název aplikace, pro kterou je PassTicket ověřen v atributu PASSTKTA definice STGCLASS fronty mostu IMS , do které má být zpráva směrována.

Pokud je hodnota PASSTKTA ponechána prázdná, musíte zajistit, aby byl vygenerován PassTicket . Název aplikace v tomto případě musí být ve formátu MVSxxxx, kde xxxx je SMFID systému z/OS , na kterém je spuštěn cílový správce front.

PassTicket je sestaven z ID uživatele, názvu cílové aplikace a tajného klíče. Jedná se o 8bajtovou hodnotu obsahující velká písmena abecedy a číselné znaky. Může být použit pouze jednou a je platný po dobu 20 minut. Je-li PassTicket generován lokálním systémem RACF , produkt RACF pouze zkontroluje, zda profil existuje, a nikoli, zda má uživatel vůči profilu oprávnění. Pokud byl PassTicket generován na vzdáleném systému, produkt RACF ověří přístup ID uživatele k profilu. Úplné informace o PassTicketsnaleznete v příručce *z/OS Security Server RACF Security Administrator's Guide*.

Záhlaví PassTickets v IMS jsou předána RACF pomocí IBM MQ, nikoli IMS.

z/OS Migrace správce front z/OS na zabezpečení s různými případy

Chcete-li migrovat správce front na zabezpečení s velkými i velkými písmeny, postupujte takto. Zkontrolujte úroveň produktu zabezpečení, který používáte, a aktivujte nové třídy externího správce zabezpečení IBM MQ . Spuštěním příkazu **REFRESH SECURITY** aktivujte profily se smíšenými písmeny.

Než začnete

1. Ujistěte se, že jsou aktivovány všechny třídy IBM MQ externího správce zabezpečení.
2. Ujistěte se, že je váš správce front spuštěn.

Informace o této úloze

Chcete-li převést správce front na zabezpečení s velkými i velkými písmeny, postupujte takto.

Postup

1. Zkopírujte všechny existující profily a úrovně přístupu z tříd velkých písmen do ekvivalentní třídy externího správce zabezpečení se smíšenými písmeny.
   a) `MQADMIN` do `MXADMIN`.
   b) `MQPROC` do `MXPROC`.
   c) `MQNLIST` do `MXNLIST`.
   d) `MQQUEUE` do `MXQUEUE`.
2. Změňte hodnotu atributu správce front `SCYCASE` na hodnotu `MIXED` zadáním následujícího příkazu.

```
ALTER QMGR SCYCASE(MIXED)
```

3. Aktivujte profily zabezpečení zadáním následujícího příkazu.

```
REFRESH SECURITY(*) TYPE(CLASSES)
```

4. Otestujte, zda vaše profily zabezpečení pracují správně.

Jak pokračovat dále

Zkontrolujte definice objektů a podle potřeby vytvořte nové profily smíšených případů pomocí příkazu **REFRESH SECURITY** , který je nezbytný pro aktivaci profilů.

Nastavení zabezpečení IBM MQ MQI client

Musíte zvážit zabezpečení systému IBM MQ MQI client , aby klientské aplikace neměly neomezený přístup k prostředkům na serveru.

Při spouštění klientské aplikace nespouštějte aplikaci s použitím ID uživatele, které má více přístupových práv, než je nezbytné; například uživatele ve skupině `mqm` nebo dokonce uživatele `mqm` .

Spuštěním aplikace jako uživatele s příliš mnoha přístupovými právy riskujete, že aplikace bude přistupovat k částem správce front a měnit je, a to buď omylem, nebo zlomyslně.

Mezi klientskou aplikací a jejím serverem správce front existují dva aspekty zabezpečení: ověřování a řízení přístupu.

- Ověření lze použít k zajištění toho, že klientská aplikace, spuštěná jako specifický uživatel, je taková, o které se říká, že je. Pomocí ověřování můžete útočníkovi zabránit v získání přístupu ke správci front zosobněním jedné z vašich aplikací.

  V produktu IBM MQ 8.0je ověření poskytováno jednou ze dvou voleb:

  – Funkce ověření připojení.

    Další informace o ověřování připojení viz “Ověření připojení” na stránce 70.

  – Použití vzájemného ověření v rámci TLS.

    Další informace o protokolu TLS viz “Práce s SSL/TLS” na stránce 276.

- Řízení přístupu lze použít k poskytnutí nebo odebrání přístupových práv pro specifického uživatele nebo skupinu uživatelů. Spuštěním klientské aplikace se specificky vytvořeným uživatelem (nebo uživatelem ve specifické skupině) pak můžete použít řízení přístupu, abyste zajistili, že aplikace nebude mít přístup k částem vašeho správce front, které by aplikace neměla mít.

  Při nastavování řízení přístupu je třeba vzít v úvahu pravidla ověřování kanálu a pole MCAUSER na kanálu. Obě tyto funkce mají schopnost změnit, které ID uživatele se používá pro ověření přístupových práv.

Další informace o řízení přístupu viz “Autorizace přístupu k objektům” na stránce 371.

Pokud jste nastavili klientskou aplikaci pro připojení ke specifickému kanálu s omezeným ID, ale kanál má v poli MCAUSER nastaveno ID administrátora, pak za předpokladu, že se klientská aplikace úspěšně připojí, použije se pro kontroly řízení přístupu ID administrátora. Proto bude mít klientská aplikace úplná přístupová práva ke správci front.

Další informace o atributu MCAUSER viz “Mapování ID uživatele klienta na ID uživatele MCAUSER” na stránce 406.

Pravidla ověřování kanálu lze také použít jako metodu řízení přístupu ke správci front nastavením specifických pravidel a kritérií pro přijetí připojení.

Další informace o pravidlech ověřování kanálu viz: “Záznamy ověření kanálu” na stránce 51.

Určení, že se za běhu v klientu MQI používají pouze specifikace CipherSpecs s certifikací FIPS.

Vytvořte úložiště klíčů pomocí softwaru vyhovujícího standardu FIPS a poté určete, že kanál musí používat specifikace CipherSpecss certifikací FIPS.

Poznámka: V systému AIX, Linux, and Windowsposkytuje produkt IBM MQ kompatibilitu se standardem FIPS 140-2 prostřednictvím šifrovacího modulu IBM Crypto for C (ICC) . Certifikát pro tento modul byl přesunut do historického stavu. Zákazníci by si měli prohlédnout IBM Crypto for C (ICC) certifikát a měli by si být vědomi všech doporučení poskytnutých NIST. Náhradní modul FIPS 140-3 momentálně probíhá a jeho stav lze zobrazit jeho vyhledáním v modulech NIST CMVP v seznamu procesů.

Aby byla úložiště klíčů za běhu kompatibilní se standardem FIPS, musí být vytvořena a spravována pouze pomocí softwaru kompatibilního se standardem FIPS, jako např. **runmqakm** s volbou `-fips` .

Můžete určit, že kanál TLS musí používat pouze specifikace CipherSpecs s certifikací FIPS, a to třemi způsoby v pořadí podle priority:

1. Nastavte pole FipsRequired ve struktuře MQSCO na hodnotu `MQSSL_FIPS_YES`.
2. Nastavte proměnnou prostředí **MQSSLFIPS** na hodnotu YES.
3. Nastavte atribut **SSLFipsRequired** v sekci SSL konfiguračního souboru klienta na hodnotu YES.

Standardně se specifikace CipherSpecs s certifikací FIPS nepožadují.

Tyto hodnoty mají stejný význam jako ekvivalentní hodnoty parametrů v systému **ALTER QMGR SSLFIPS** (viz **ALTER QMGR** (změna nastavení správce front)). Pokud proces klienta aktuálně nemá aktivní připojení TLS a hodnota FipsRequired je v souboru MQCONNX zabezpečení SSL zadána platně, musí všechna následná připojení TLS přidružená k tomuto procesu používat pouze specifikace CipherSpecs přidružené k této hodnotě. To platí až do zastavení tohoto a všech ostatních připojení TLS, kdy následné připojení MQCONNX může poskytnout novou hodnotu pro FipsRequired.

Je-li přítomen kryptografický hardware, šifrovací moduly používané produktem IBM MQ lze konfigurovat tak, aby byly moduly poskytované hardwarovým produktem, a tyto moduly mohou být certifikovány podle standardu FIPS na konkrétní úroveň. Konfigurovatelné moduly a to, zda mají certifikaci FIPS, závisí na používaném hardwarovém produktu.

Kde je to možné, je-li nakonfigurováno CipherSpecs pouze se standardem FIPS, klient MQI odmítne připojení, která určují jinou specifikaci než FIPS CipherSpec s volbou `MQRC_SSL_INITIALIZATION_ERROR`. Produkt IBM MQ nezaručuje, že odmítne všechna taková připojení, a je vaší odpovědností určit, zda je konfigurace produktu IBM MQ kompatibilní s FIPS.

Související pojmy

“Standard FIPS (Federal Information Processing Standards) pro AIX, Linux, and Windows” na stránce 34
Je-li v systémech AIX, Linux, and Windows vyžadováno šifrování v kanálu SSL/TLS, používá produkt IBM MQ šifrovací balík s názvem IBM Crypto for C (ICC). Na platformách AIX, Linux, and Windows prošel software ICC programem FIPS (Federal Information Processing Standards) Cryptomodule Validation Program amerického Národního institutu pro standardy a technologie (US National Institute of Standards and Technology) na úrovni 140-2.

AIX Spuštění aplikací klienta TLS s více instalacemi produktu GSKit 8.0 na systému AIX

Klientské aplikace TLS v systému AIX se mohou vyskytnout MQRC_CHANNEL_CONFIG_ERROR a chyba AMQ6175 při spuštění na systémech AIX s více instalacemi produktu IBM Global Security Kit (GSKit) verze 8.0 .

Při spouštění aplikací klienta v systému AIX s více instalacemi produktu GSKit 8.0 mohou volání připojení klienta vrátit hodnotu MQRC_CHANNEL_CONFIG_ERROR při použití protokolu TLS. /var/mqm/errors Chyba záznamu protokolu AMQ6175 a AMQ9220 pro selhávající klientskou aplikaci, například:

```
09/08/11 11:16:13 - Process(24412.1) User(user) Program(example)
Host(machine.example.ibm.com) Installation(Installation1)
VRMF(7.1.0.0)
AMQ6175: The system could not dynamically load the shared library
'/usr/mqm/gskit8/lib64/libgsk8ssl_64.so'. The system returned
error number '8' and error message 'Symbol resolution failed
for /usr/mqm/gskit8/lib64/libgsk8ssl_64.so because:
Symbol VALUE_EC_NamedCurve_secp256r1__9GSKASNOID (number 16) is not
exported from dependent module /db2data/db2inst1/sqllib/lib64/libgsk8cms_64.so.
Symbol VALUE_EC_NamedCurve_secp384r1__9GSKASNOID (number 17) is not exported from
dependent module /db2data/db2inst1/sqllib/lib64/libgsk8cms_64.so.
Symbol VALUE_EC_NamedCurve_secp521r1__9GSKASNOID (number 18) is not exported from
dependent module /db2data/db2inst1/sqllib/lib64/libgsk8cms_64.so.
Symbol VALUE_EC_ecPublicKey__9GSKASNOID (number 19) is not exported from dependent
module /db2data/db2inst1/sqllib/lib64/libgsk8cms_64.so.
Symbol VALUE_EC_ecdsa_with_SHA1__9GSKASNOID (number 20) is not exported from
dependent module /db2data/db2inst1/sqllib/lib64/libgsk8cms_64.so.
Symbol VALUE_EC_ecdsa__9GSKASNOID (number 21) is not exported from dependent
module /db2data/db2inst1/sqllib/lib64/libgsk8cms_64.so.'.

EXPLANATION:
This message applies to AIX systems. The shared library
'/usr/mqm/gskit8/lib64/libgsk8ssl_64.so' failed
to load correctly due to a problem with the library.
ACTION:
Check the file access permissions and that the file has not been corrupted.
----- amqxufnx.c : 1284 ---------------------------------------------------------
09/08/11 11:16:13 - Process(24412.1) User(user) Program(example)
Host(machine.example.ibm.com) Installation(Installation1)
VRMF(7.1.0.0)
AMQ9220: The GSKit communications program could not be loaded.

EXPLANATION:
The attempt to load the GSKit library or procedure
'/usr/mqm/gskit8/lib64/libgsk8ssl_64.so' failed with error code
536895861.
ACTION:
Either the library must be installed on the system or the environment changed
to allow the program to locate it.
----- amqcgska.c : 836 ----------------------------------------------------------
```

Běžnou příčinou této chyby je, že nastavení proměnné prostředí LIBPATH nebo LD_LIBRARY_PATH způsobilo, že klient IBM MQ načetl smíšenou sadu knihoven ze dvou různých instalací produktu GSKit 8.0 . Provedení aplikace klienta IBM MQ v prostředí Db2 může způsobit tuto chybu.

Chcete-li se vyhnout této chybě, zahrňte adresáře knihoven IBM MQ na přední straně cesty ke knihovně tak, aby knihovny IBM MQ byly přednostní. Toho lze dosáhnout pomocí příkazu **setmqenv** s parametrem **-k** , například:

```
. /usr/mqm/bin/setmqenv -s -k
```

Další informace o použití příkazu **setmqenv** naleznete v příručce setmqenv (set IBM MQ environment) .

Konfigurace kanálů TLS pomocí MQSC

Chcete-li konfigurovat kanály TLS, použijte příkazy **runmqsc** a ALTER CHANNEL. Kanál můžete volitelně konfigurovat tak, aby přijímal pouze certifikáty s atributy v rozlišujícím názvu vlastníka, které odpovídají

zadaným hodnotám. Volitelně můžete též konfigurovat kanál správce front tak, aby správce front odmítl připojení v případě, že inicializující strana neodešle vlastní osobní certifikát.

Informace o této úloze

Chcete-li nakonfigurovat kanály v produktu IBM MQ Explorer, prohlédněte si téma Konfigurace kanálů TLS pomocí produktu IBM MQ Explorer.

Chcete-li nakonfigurovat kanály pomocí produktu **runmqsc**, postupujte takto.

Postup

1. Vyvolejte příkaz **runmqsc** , který se připojuje k cílovému správci front.
2. Identifikujte kanál, který chcete povolit pro TLS.

   Poznamenejte si název kanálu i typ kanálu.
3. Pomocí příkazu ALTER CHANNEL můžete změnit různé vlastnosti kanálu IBM MQ .

   Kromě příkazu zadejte název kanálu a typ kanálu. Chcete-li například změnit kanál odesilatele s názvem MQ.TEST spusťte následující příkaz:

   ```
   ALTER CHANNEL(‘MQ.TEST’) CHLTYPE(SDR)
   ```

   Existují různé atributy kanálu související s protokolem TLS, které můžete upravit v definicích kanálu IBM MQ .

Jak pokračovat dále

Nastavení zabezpečení zpráv

Systém zpráv se zabezpečením TLS nabízí dvě metody pro zabezpečení zpráv:

- Díky šifrování je zajištěno, že zpráva je při případném zachycení nečitelná.
- Díky funkcím typu hash lze odhalit případný zásah do integrity zpráv.

Kombinace těchto dvou metod je označována termínem specifikace CipherSpec. Pro oba konce kanálu musí být nastavena stejná specifikace CipherSpec, jinak systém zpráv s povoleným zabezpečením TLS selže. Další informace viz téma “zabezpečeníIBM MQ” na stránce 7.

Chcete-li změnit protokol TLS pro povolení kanálu IBM MQ , zadejte hodnotu do atributu SSLCIPH. Tento atribut musí být nastaven na platnou specifikaci CipherSpec pro platformu fronty správce front ze seznamu “Povolení CipherSpecs” na stránce 438.

Chcete-li změnit kanál IBM MQ tak, aby zakázal protokol TLS, nastavte parametr SSLCIPH na prázdnou hodnotu. Příklad:

```
ALTER CHANNEL(‘MQ.TEST’) CHLTYPE(SDR) SSLCIPH(ANY_TLS12_OR_HIGHER)
```

Poznámka: Musíte uzavřít název kanálu do apostrofů, abyste se ujistili, že jsou zachována malá a velká písmena. Bez apostrofů produkt IBM MQ transformuje řetězec na velká písmena.

Filtrování certifikátů podle jmen vlastníků

Certifikáty obsahují rozlišující název svého vlastníka. Kanál můžete volitelně konfigurovat tak, aby přijímal pouze certifikáty s atributy v rozlišujícím názvu vlastníka, které odpovídají zadaným hodnotám.

Názvy atributů, které může produkt IBM MQ filtrovat, jsou uvedeny v následující tabulce:

Názvy atributů	**Význam**
SERIALNUMBER	Sériové číslo certifikátu
MAIL	E-mailová adresa
Deprecated E	E-mailová adresa (zamítnuto ve prospěch volby MAIL)

Názvy atributů	Význam
UID nebo USERID	Identifikátor uživatele
CN	Obecný název
T	Titulek
OU	Název organizační jednotky
DC	Komponenta domény
O	Název organizace
STREET	Ulice/první řádek adresy
L	Název umístění
ST (nebo SP či S)	Název státu nebo správního celku
Osobní počítač	PSČ
C	Země
UNSTRUCTUREDNAME	Název hostitele
UNSTRUCTUREDADDRESS	Adresa IP
DNQ	Kvalifikátor rozlišujícího názvu

Místo libovolného počtu znaků můžete použít zástupný znak (*) na začátku nebo na konci hodnoty atributu. Chcete-li například přijímat pouze certifikáty od osob, jejichž jméno končí na `Smith` a které pracují pro společnost `IBM` v zemi `GB`, zadejte:

```
CN=*Smith, O=IBM, C=GB
```

Příklad:

```
ALTER CHANNEL('MQ.TEST') CHLTYPE(SDR) SSLPEER('CN=*Smith, O=IBM, C=GB')
```

Poznámka: Musíte uzavřít řetězec SSLPEER do apostrofů, abyste se ujistili, že je zachována velikost písmen. Bez apostrofů produkt IBM MQ transformuje řetězec na velká písmena.

Ověřování stran inicializujících připojení ke správci front

Pokud připojení s povoleným zabezpečením ke správci front inicializuje jiná strana, musí správce front inicializující straně odeslat jako důkaz identity osobní certifikát. Volitelně můžete též konfigurovat kanál správce front tak, aby správce front odmítl připojení v případě, že inicializující strana neodešle vlastní osobní certifikát.

Chcete-li tak učinit, nastavte atribut SSLCAUTH. Tento atribut je logickým atributem a může mít hodnoty OPTIONAL nebo REQUIRED:

- VOLITELNĚ ověřuje certifikát připojujícího se klienta, je-li poskytnut, ale nevyžaduje, aby jej klient odeslal. Klient je odmítnut, pokud odešle neplatný certifikát.
- REQUIRED zamítne všechny připojující se klienty, kteří neposkytují platný certifikát TLS

Příklad:

```
ALTER CHANNEL('MQ.TEST') CHLTYPE(SDR) SSLCAUTH(REQUIRED)
```

IBM i Nastavení komunikací pro zabezpečení SSL nebo TLS na systému IBM i

Zabezpečené komunikace, které používají šifrovací protokoly zabezpečení SSL nebo TLS, zahrnují nastavení komunikačních kanálů a správu digitálních certifikátů, které budete používat pro ověření.

Chcete-li nastavit instalaci SSL nebo TLS, musíte definovat kanály pro použití SSL nebo TLS. Musíte také vytvořit a spravovat své digitální certifikáty. V některých operačních systémech můžete provádět testy s certifikáty podepsanými sebou samým. V systému IBM ivšak musíte používat osobní certifikáty podepsané lokální CA.

Úplné informace o vytváření a správě certifikátů naleznete v části "Práce se zabezpečením SSL/TLS v systému IBM i" na stránce 276.

Tato kolekce témat představuje některé úlohy, které se podílejí na nastavení komunikace SSL nebo TLS, a poskytuje podrobné pokyny k provádění těchto úloh.

Můžete také testovat ověření klienta SSL nebo TLS, což jsou volitelné části protokolů SSL a TLS. Během komunikace výměnou potvrzení SSL nebo TLS klient SSL nebo TLS vždy získá a ověří digitální certifikát ze serveru. S implementací IBM MQ si server SSL nebo TLS vždy vyžádá certifikát od klienta.

V systému IBM iklient SSL nebo TLS odešle certifikát pouze v případě, že má certifikát označený ve správném formátu IBM MQ :

- V případě správce front se hodnota `ibmwebspheremq` následovaná názvem správce front změnila na malá písmena. Například pro `QM1`, `ibmwebspheremqqm1`.
- V případě klienta IBM MQ C pro IBM i `ibmwebspheremq` se ID uživatele pro přihlášení změnilo na malá písmena, například `ibmwebspheremqmyuserid`.

Produkt IBM MQ používá předponu `ibmwebspheremq` na štítku, aby se zabránilo záměně s certifikáty pro jiné produkty. Ujistěte se, že jste zadali celý popisek certifikátu malými písmeny.

Server SSL nebo TLS vždy ověří certifikát klienta, pokud je odeslán. Pokud klient SSL nebo TLS neodešle certifikát, ověření se nezdaří pouze v případě, že je konec kanálu, který vystupuje jako server SSL nebo TLS, definován buď s parametrem SSLCAUTH nastaveným na hodnotu REQUIRED, nebo s hodnotou parametru SSLPEER. Další informace naleznete v tématu Připojení dvou správců front pomocí zabezpečení SSL nebo TLS.

ALW Nastavení komunikací pro zabezpečení SSL nebo TLS na systému AIX, Linux, and Windows

Zabezpečené komunikace, které používají šifrovací protokoly zabezpečení SSL nebo TLS, zahrnují nastavení komunikačních kanálů a správu digitálních certifikátů, které budete používat pro ověření.

Chcete-li nastavit instalaci SSL nebo TLS, musíte definovat kanály pro použití SSL nebo TLS. Musíte také vytvořit a spravovat své digitální certifikáty. Na systémech AIX, Linux, and Windows můžete provádět testy s certifikáty podepsanými sebou samým.

Upozornění: U správců front, které chcete spojit pomocí kanálů s povoleným protokolem TLS, nelze použít kombinaci certifikátů podepsaných pomocí eliptické křivky a certifikátů podepsaných pomocí protokolu RSA.

Všichni správci front používající kanály s povoleným protokolem TLS musí používat certifikáty podepsané RSA, nebo všichni používají certifikáty podepsané EC, nikoli kombinaci obojího.

Další informace viz "Digitální certifikáty a kompatibilita CipherSpec v produktu IBM MQ" na stránce 46.

Certifikáty podepsané svým držitelem nelze odvolat, což by mohlo útočníkovi umožnit zfalšovat identitu poté, co byl ohrožen soukromý klíč. Certifikační autority mohou odvolat ohrožený certifikát, což brání jeho dalšímu použití. Certifikáty podepsané certifikační autoritou jsou proto bezpečnější pro použití v produkčním prostředí, ačkoli certifikáty podepsané sebou samým jsou pro testovací systém pohodlnější.

Úplné informace o vytváření a správě certifikátů naleznete v části “Práce se zabezpečením SSL/TLS v systému AIX, Linux, and Windows” na stránce 293.

Tato kolekce témat představuje některé úlohy, které se podílejí na nastavení komunikace SSL, a poskytuje podrobné pokyny k provádění těchto úloh.

Můžete také testovat ověření klienta SSL nebo TLS, které jsou volitelnou součástí protokolů. Během komunikace výměnou potvrzení SSL nebo TLS klient SSL nebo TLS vždy získá a ověří digitální certifikát ze serveru. S implementací IBM MQ si server SSL nebo TLS vždy vyžádá certifikát od klienta.

V systému AIX, Linux, and Windowsklient SSL nebo TLS odešle certifikát pouze v případě, že má certifikát označený ve správném formátu IBM MQ :

- Pro správce front je formát `ibmwebspheremq` následován názvem správce front, který byl změněn na malá písmena. Například pro `QM1`, `ibmwebspheremqqm1`
- V případě klienta IBM MQ `ibmwebspheremq` následovaného ID uživatele pro přihlášení se změnilo na malá písmena, například `ibmwebspheremqmyuserid`.

Produkt IBM MQ používá předponu `ibmwebspheremq` na štítku, aby se zabránilo záměně s certifikáty pro jiné produkty. Ujistěte se, že jste zadali celý popisek certifikátu malými písmeny.

Server SSL nebo TLS vždy ověří certifikát klienta, pokud je odeslán. Pokud klient neodešle certifikát, ověření se nezdaří pouze v případě, že je konec kanálu, který vystupuje jako server SSL nebo TLS, definován buď s parametrem SSLCAUTH nastaveným na hodnotu REQUIRED, nebo s hodnotou parametru SSLPEER. Další informace naleznete v tématu Připojení dvou správců front pomocí zabezpečení SSL nebo TLS.

z/OS Nastavení komunikací pro zabezpečení SSL nebo TLS na systému z/OS

Zabezpečené komunikace, které používají šifrovací protokoly zabezpečení SSL nebo TLS, zahrnují nastavení komunikačních kanálů a správu digitálních certifikátů, které budete používat pro ověření.

Chcete-li nastavit instalaci SSL nebo TLS, musíte definovat kanály pro použití SSL nebo TLS. Musíte také vytvořit a spravovat své digitální certifikáty. V systému z/OS můžete provádět testy s certifikáty podepsanými držitelem nebo s osobními certifikáty podepsanými lokální certifikační autoritou (CA).

Certifikáty podepsané svým držitelem nelze odvolat, což by mohlo útočníkovi umožnit zfalšovat identitu poté, co byl ohrožen soukromý klíč. Certifikační autority mohou odvolat ohrožený certifikát, což brání jeho dalšímu použití. Certifikáty podepsané certifikační autoritou jsou proto bezpečnější pro použití v produkčním prostředí, ačkoli certifikáty podepsané sebou samým jsou pro testovací systém pohodlnější.

Úplné informace o vytváření a správě certifikátů naleznete v části “Práce se zabezpečením SSL/TLS v systému z/OS” na stránce 331.

Další informace viz parametry CERTLABL a CERTQSGL příkazu ALTER QMGR a parametr CERLABL příkazu DEFINE CHANNEL .

Pořadí přednosti je:

- parametr CERTLABL kanálu
- Parametr QMGR CERTQSGL, pokud je kanál sdílený.

  Pro kanál odesilatele to znamená, že přenosová fronta (XMITQ) je sdílená. Pro přijímací kanál to znamená kanál spuštěný prostřednictvím sdíleného modulu listener, tj. modul listener s INDISP (GROUP).
- QMGR CERTLABL
- Výchozí popisek `ibmWebSphereMQ` následovaný názvem skupiny sdílení front pro sdílené kanály nebo názvem správce front.

Tato kolekce témat představuje některé úlohy, které se podílejí na nastavení komunikace SSL nebo TLS, a poskytuje podrobné pokyny k provádění těchto úloh.

Můžete také testovat ověření klienta SSL nebo TLS, které jsou volitelnou součástí protokolů. Během komunikace výměnou potvrzení SSL nebo TLS klient SSL nebo TLS vždy získá a ověří digitální certifikát ze serveru. S implementací IBM MQ si server SSL nebo TLS vždy vyžádá certifikát od klienta.

Pokud je kanál sdílený, kanál se nejprve pokusí najít certifikát pro skupinu sdílení front. Pokud nenalezne certifikát pro skupinu sdílení front, pokusí se najít certifikát pro správce front.

V systému z/OSpoužívá produkt IBM MQ předponu `ibmWebSphereMQ` na štítku, aby se zabránilo záměně s certifikáty pro jiné produkty.

Server SSL nebo TLS vždy ověří certifikát klienta, pokud je odeslán. Pokud klient SSL nebo TLS neodešle certifikát, ověření se nezdaří pouze v případě, že je konec kanálu, který vystupuje jako server SSL nebo TLS, definován buď s parametrem SSLCAUTH nastaveným na hodnotu REQUIRED, nebo s hodnotou parametru SSLPEER. Další informace naleznete v tématu Připojení dvou správců front pomocí zabezpečení SSL nebo TLS.

Práce s SSL/TLS

Tato témata poskytují pokyny pro provádění jednotlivých úloh souvisejících s použitím TLS s produktem IBM MQ.

Mnohé z nich se používají jako kroky v úlohách vyšší úrovně popsaných v následujících sekcích:

- “Identifikace a ověřování uživatelů” na stránce 343
- “Autorizace přístupu k objektům” na stránce 371
- “Důvěrnost zpráv” na stránce 437
- “Integrita dat zpráv” na stránce 494
- “Zachování zabezpečení klastrů” na stránce 495

IBM i Práce se zabezpečením SSL/TLS v systému IBM i

Tato kolekce témat poskytuje pokyny pro jednotlivé úlohy pracující s protokolem TLS (Transport Layer Security) v produktu IBM MQ for IBM i.

Pro systém IBM i je podpora TLS nedílnou součástí operačního systému. Ujistěte se, že jste nainstalovali předpoklady uvedené v části Požadavky na hardware a software na systému IBM i.

V systému IBM ispravujete klíče a digitální certifikáty pomocí nástroje DCM (Digital Certificate Manager).

Přístup k produktu DCM

Postupujte podle těchto pokynů pro přístup k rozhraní DCM.

Informace o této úloze

Ve webovém prohlížeči, který podporuje rámce, proveďte následující kroky.

Postup

1. Přejděte na `http://machine.domain:2001` nebo `https://machine.domain:2010`, kde *počítač* je název vašeho počítače.
2. Na požádání zadejte platný profil uživatele a heslo.

   Ujistěte se, že váš profil uživatele má speciální oprávnění *ALLOBJ a *SECADM, abyste mohli vytvářet nová úložiště certifikátů. Pokud nemáte speciální oprávnění, můžete spravovat pouze osobní certifikáty nebo zobrazit podpisy objektů pro objekty, pro které máte oprávnění. Máte-li oprávnění používat aplikaci pro podepisování objektů, můžete také podepisovat objekty z produktu DCM.
3. Na stránce Konfigurace Internetu klepněte na volbu **Digitální Certificate Manager**.

   Zobrazí se stránka Digital Certificate Manager .

Přiřazení certifikátu ke správci front v systému IBM i

Pomocí produktu DCM můžete přiřadit certifikát ke správci front.

K přiřazení certifikátu ke správci front použijte tradiční správu digitálních certifikátů IBM i . To znamená, že můžete určit, že správce front používá úložiště certifikátů systému a že je správce front registrován pro použití jako aplikace v produktu Digital Certificate Manager. Chcete-li tak učinit, změňte hodnotu atributu **SSLKEYR** správce front na *SYSTEM.

Je-li parametr **SSLKEYR** změněn na hodnotu *SYSTEM, produkt IBM MQ zaregistruje správce front jako serverovou aplikaci s jedinečným popiskem aplikace QIBM_WEBSPHERE_MQ_QMGRNAME a popiskem s popisem Qmgrname (WMQ). Všimněte si, že atributy kanálu **CERTLABL** se nepoužívají, pokud používáte úložiště certifikátů *SYSTEM. Správce front se poté zobrazí jako serverová aplikace v produktu Digital Certificate Managera k této aplikaci můžete přiřadit libovolný certifikát serveru nebo klienta v systémovém úložišti.

Protože je správce front registrován jako aplikace, lze provádět rozšířené funkce produktu DCM, jako např. definování seznamů důvěryhodných CA.

Pokud je parametr **SSLKEYR** změněn na jinou hodnotu než *SYSTEM, IBM MQ odregistruje správce front jako aplikaci pomocí produktu Digital Certificate Manager. Dojde-li k odstranění správce front, bude také zrušena jeho registrace v produktu DCM. Uživatel s dostatečným oprávněním *SECADM může také ručně přidávat nebo odebírat aplikace z produktu DCM.

Nastavení úložiště klíčů v systému IBM i

Úložiště klíčů musí být nastaveno na obou koncích připojení. Výchozí úložiště certifikátů lze použít nebo si můžete vytvořit vlastní.

Připojení TLS vyžaduje na každém konci připojení *úložiště klíčů* . Každý správce front a produkt IBM MQ MQI client musí mít přístup k úložišti klíčů. Chcete-li přistupovat k úložišti klíčů pomocí názvu souboru a hesla (tj. bez použití volby *SYSTEM), ujistěte se, že profil uživatele QMQM má následující oprávnění:

- Oprávnění ke spuštění pro adresář obsahující úložiště klíčů
- Oprávnění ke čtení pro soubor obsahující úložiště klíčů

Další informace viz “Úložiště klíčů SSL/TLS” na stránce 25. Všimněte si, že atributy kanálu **CERTLABL** se nepoužívají, pokud používáte paměť certifikátů *SYSTEM.

V systému IBM ijsou digitální certifikáty uloženy v úložišti certifikátů, které je spravováno pomocí produktu DCM. Tyto digitální certifikáty mají jmenovky, které přidružují certifikát ke správci front nebo k produktu IBM MQ MQI client. TLS používá certifikáty pro účely ověření.

Popisek je buď hodnota atributu **CERTLABL** , je-li nastaven, nebo výchozí hodnota `ibmwebspheremq` s připojeným názvem správce front nebo ID přihlášení uživatele IBM MQ MQI client , vše malými písmeny. Podrobnosti viz Popisky digitálních certifikátů .

Název správce front nebo úložiště certifikátů IBM MQ MQI client obsahuje cestu a název kmene. Výchozí cesta je `/QIBM/UserData/ICSS/Cert/Server/` a výchozí název kmene je `Default`. V systému IBM ije výchozí úložiště certifikátů `/QIBM/UserData/ICSS/Cert/Server/Default.kdb`také známé jako *SYSTEM. Volitelně můžete definovat vlastní cestu a název kmene.

Pokud definujete vlastní cestu nebo název souboru, nastavte oprávnění k souboru, abyste k němu pevně řídili přístup.

“Změna umístění úložiště klíčů pro správce front v systému IBM i” na stránce 280 vám sdělí, jak zadat název úložiště certifikátů. Název úložiště certifikátů můžete zadat buď před, nebo po vytvoření úložiště certifikátů.

Poznámka: Operace, které můžete provádět s produktem DCM, mohou být omezeny oprávněním vašeho uživatelského profilu. K vytvoření certifikátu CA například potřebujete oprávnění *ALLOBJ a *SECADM.

V 9.3.0 IBM i V 9.3.0 *Šifrování hesel úložiště klíčů v systému IBM i*

Několik komponent produktu IBM MQ potřebuje přístup k úložišti klíčů, které obsahuje digitální certifikáty nebo symetrické klíče. Úložiště klíčů je zabezpečeno heslem, protože obsahuje citlivé informace. Heslo

úložiště klíčů musí být uloženo v umístění, kde jej může produkt IBM MQ číst při přístupu k úložišti klíčů. Heslo musí být také zašifrováno, aby se snížila pravděpodobnost neoprávněného přístupu k úložišti klíčů.

Následující komponenty a funkce produktu IBM MQ podporují dvě různé metody ukládání hesel úložiště klíčů:

- Úložiště klíčů TLS správce front.
- IBM MQ MQI clients , které používají TLS.

Hesla úložiště klíčů pro použití těmito komponentami jsou chráněna pomocí systému ochrany hesel produktu IBM MQ . Mechanismus pro zadání hesla a jeho šifrování se mírně liší v závislosti na komponentě:

Úložiště klíčů TLS správce front

Heslo je šifrováno při nastavení atributu správce front **SSLKEYRPWD** pomocí příkazu CHGMQM (Change Message Queue Manager) .

Heslo je šifrováno pomocí algoritmu AES-128 . Podrobnosti tohoto algoritmu jsou veřejně známé a jsou považovány za bezpečné.

Heslo je uloženo v souboru pro dočasné ukládání v proprietárním formátu, který není chápán jiným softwarem, který by mohl přistupovat k úložišti klíčů.

Heslo, které je šifrováno jednou komponentou IBM MQ , nemůže být použito jinou komponentou IBM MQ .

Při šifrování hesla úložiště klíčů lze poskytnout jedinečný šifrovací klíč. Jedinečný šifrovací klíč zabraňuje každému, kdo nemá přístup k šifrovacímu klíči, aby mohl dešifrovat heslo. Tento klíč zadáváte prostřednictvím atributu správce front **INITKEY** , který musí být nastaven před zadáním hesla, které má být šifrováno.

Další informace o systému IBM MQ pro ochranu heslem naleznete v části “Ochrana hesel v konfiguračních souborech komponenty IBM MQ” na stránce 580.

IBM MQ MQI clients , které používají TLS

Produkt “IBM MQ Obslužný program klienta SSL (amqrsslc) pro IBM i” na stránce 291 může uložit heslo úložiště klíčů do souboru pro dočasné ukládání. Viz také téma Administrace pomocí příkazů MQSC na systému IBM i.

Heslo je šifrováno pomocí algoritmu AES-128 . Podrobnosti tohoto algoritmu jsou veřejně známé a jsou považovány za bezpečné.

Heslo je uloženo v souboru pro dočasné ukládání v proprietárním formátu, který není chápán jiným softwarem, který by mohl přistupovat k úložišti klíčů.

Při šifrování hesla úložiště klíčů lze poskytnout jedinečný šifrovací klíč. Jedinečný šifrovací klíč zabraňuje každému, kdo nemá přístup k šifrovacímu klíči, aby mohl dešifrovat heslo. Tento klíč zadáte prostřednictvím parametru **-sf** .

Šifrované heslo je uloženo v souboru pro dočasné ukládání ve stejném adresáři jako soubor úložiště klíčů.

Produkt IBM MQ MQI clients také podporuje hesla poskytovaná prostřednictvím jiných mechanismů. Viz téma “Zadání hesla úložiště klíčů pro IBM MQ MQI client on IBM i” na stránce 281.

Bez ohledu na metodu, kterou zvolíte pro šifrování hesla úložiště klíčů, se ujistěte, že jste si vědomi omezení šifrování uložených hesel. Viz “Omezení ochrany pomocí šifrování hesla” na stránce 588.

Související pojmy

“Zadání hesla úložiště klíčů pro správce front v systému IBM i” na stránce 281
Protože úložiště klíčů obsahuje citlivé informace, je zabezpečeno heslem. Chcete-li mít přístup k obsahu úložiště klíčů za účelem provádění operací TLS, musí být produkt IBM MQ schopen načíst heslo úložiště klíčů.

“Zadání hesla úložiště klíčů pro IBM MQ MQI client on IBM i” na stránce 281

Protože úložiště klíčů obsahuje citlivé informace, je zabezpečeno heslem. Chcete-li mít přístup k obsahu úložiště klíčů za účelem provádění operací TLS, musí být produkt IBM MQ schopen načíst heslo úložiště klíčů.

“Práce se zabezpečením SSL/TLS v systému IBM i” na stránce 276
Tato kolekce témat poskytuje pokyny pro jednotlivé úlohy pracující s protokolem TLS (Transport Layer Security) v produktu IBM MQ for IBM i.

Vytvoření úložiště certifikátů v systému IBM i
Pokud nechcete použít výchozí úložiště certifikátů, postupujte podle tohoto postupu a vytvořte si vlastní.

Informace o této úloze

Nové úložiště certifikátů vytvořte pouze v případě, že nechcete používat výchozí úložiště certifikátů IBM i .

Chcete-li určit, že má být použito úložiště certifikátů systému IBM i , změňte hodnotu atributu SSLKEYR správce front na hodnotu *SYSTEM. Tato hodnota označuje, že správce front používá úložiště certifikátů systému a správce front je registrován pro použití jako aplikace s produktem DCM (Digital Certificate Manager).

Postup

1. Přístup k rozhraní DCM, jak je popsáno v tématu “Přístup k produktu DCM” na stránce 276 .
2. V navigačním panelu klepněte na volbu **Vytvořit nové úložiště certifikátů**.
   V rámci úlohy se zobrazí stránka Vytvořit nové úložiště certifikátů.
3. V rámci úlohy vyberte volbu **Jiné systémové úložiště certifikátů** a klepněte na tlačítko **Pokračovat**.
   V rámci úlohy se zobrazí stránka Vytvořit certifikát v novém úložišti certifikátů.
4. Vyberte volbu **Ne-nevytvářet certifikát v úložišti certifikátů** a klepněte na tlačítko **Pokračovat**.
   V rámci úlohy se zobrazí stránka Název a heslo úložiště certifikátů.
5. Do pole **Cesta a název souboru úložiště certifikátů** zadejte cestu IFS a název souboru, například `/QIBM/UserData/mqm/qmgrs/qm1/key.kdb` .
6. Zadejte heslo do pole **Heslo** a zadejte je znovu do pole **Potvrdit heslo** . Klepněte na tlačítko **Pokračovat**.
   Poznamenejte si heslo (které rozlišuje velká a malá písmena), protože je potřebujete při ukládání klíče úložiště.
7. Chcete-li ukončit produkt DCM, zavřete okno prohlížeče.

Jak pokračovat dále

Po vytvoření úložiště certifikátů pomocí produktu DCM se ujistěte, že jste heslo uložili, jak je popsáno v tématu “Uložení hesla úložiště certifikátů na systémech IBM i” na stránce 279 .

Související úlohy

“Import certifikátu do úložiště klíčů v systému IBM i” na stránce 289
Chcete-li importovat certifikát, postupujte podle této procedury.

Uložení hesla úložiště certifikátů na systémech IBM i
Uložte heslo úložiště certifikátů pomocí příkazů CL.

Následující pokyny se vztahují na ukládání hesla úložiště certifikátů v systému IBM i pro správce front. Alternativně pro systém IBM MQ MQI client, pokud nepoužíváte úložiště certifikátů *SYSTEM (tj. prostředí MQSSLKEYR je nastaveno na jinou hodnotu než *SYSTEM), postupujte podle procedury popsané v “Uložit heslo úložiště certifikátů” na stránce 292 části “IBM MQ Obslužný program klienta SSL (amqrsslc) pro IBM i” na stránce 291.

Pokud jste uvedli, že se má použít úložiště certifikátů *SYSTEM (změnou hodnoty atributu SSLKEYR správce front na *SYSTEM), nesmíte postupovat takto.

Po vytvoření úložiště certifikátů pomocí produktu DCM použijte k uložení hesla následující příkazy:

```
STRMQM MQMNAME('queue_manager_name')
CHGMQM MQMNAME('queue_manager_name') SSLKEYRPWD('password')
```

V heslu se rozlišují malá a velká písmena. Musí být zadán v apostrofech přesně tak, jak jste jej zadali v kroku 6 “Vytvoření úložiště certifikátů v systému IBM i” na stránce 279.

Poznámka: Pokud nepoužíváte výchozí systémové úložiště certifikátů a heslo neuchováváte, pokusy o spuštění kanálů TLS se nezdaří, protože nemohou získat heslo požadované pro přístup k úložišti certifikátů.

Ochrana pomocí hesla

V 9.3.0

Je-li zadáno heslo úložiště klíčů, produkt IBM MQ heslo zašifruje pomocí systému IBM MQ Password Protection. Chcete-li zašifrovat heslo, použije se počáteční klíč. Není-li tento klíč dodán správci front, použije se místo něj výchozí klíč.

Před zadáním hesla úložiště klíčů byste měli nastavit jedinečný počáteční klíč pro správce front. To lze provést pomocí atributu **INITKEY** příkazu **ALTER QMGR** MQSC:

```
ALTER QMGR INITKEY('value')
```

Vyhledání úložiště klíčů pro správce front v systému IBM i

Tento postup použijte k získání umístění úložiště certifikátů vašeho správce front.

Postup

1. Zobrazte atributy správce front pomocí následujícího příkazu:

   ```
   DSPMQM MQMNAME('queue manager name')
   ```

2. Zkontrolujte výstup příkazu pro cestu a název kmene úložiště certifikátů.

   Například: `/QIBM/UserData/ICSS/Cert/Server/Default`, kde `/QIBM/UserData/ICSS/Cert/Server` je cesta a `Default` je název kmene.

Změna umístění úložiště klíčů pro správce front v systému IBM i

Změňte umístění úložiště certifikátů správce front pomocí příkazu CHGMQM nebo ALTER QMGR.

Postup

K nastavení atributu úložiště klíčů správce front použijte buď příkaz CHGMQM, nebo příkaz ALTER QMGR MQSC.

a) Použití příkazu CHGMQM: `CHGMQM MQMNAME('qm1') SSLKEYR('/QIBM/UserData/ICSS/Cert/Server/MyKey.kdb')`

b) Použití příkazu ALTER QMGR: `ALTER QMGR SSLKEYR('/QIBM/UserData/ICSS/Cert/Server/MyKey.kdb')`

V obou případech má úložiště certifikátů úplný název souboru: `/QIBM/UserData/ICSS/Cert/Server/MyKey.kdb`

Jak pokračovat dále

Změníte-li umístění úložiště certifikátů správce front, certifikáty nebudou přeneseny ze starého umístění. Pokud jsou certifikáty CA předinstalované při vytváření úložiště certifikátů nedostatečné, musíte naplnit nové úložiště certifikátů certifikáty, jak je popsáno v tématu “Import certifikátu do úložiště klíčů v systému IBM i” na stránce 289. Heslo pro nové umístění musíte také schovat, jak je popsáno v tématu “Uložení hesla úložiště certifikátů na systémech IBM i” na stránce 279.

V 9.3.0 IBM i V 9.3.0 *Zadání hesla úložiště klíčů pro správce front v systému IBM i*

Protože úložiště klíčů obsahuje citlivé informace, je zabezpečeno heslem. Chcete-li mít přístup k obsahu úložiště klíčů za účelem provádění operací TLS, musí být produkt IBM MQ schopen načíst heslo úložiště klíčů.

Produkt IBM MQ poskytuje mechanizmus pro zadání hesla úložiště klíčů správci front:

- Parametr **SSLKEYRPWD** v příkazu **CHGMQM**

Heslo úložiště klíčů je šifrováno pomocí systému ochrany hesla IBM MQ . Další informace o metodách ochrany hesla úložiště klíčů viz “Šifrování hesel úložiště klíčů v systému IBM i” na stránce 277.

Viz také téma Administrace použití příkazů MQSC na systému IBM i.

Atribut SSLKEYRPWD

Chcete-li zadat heslo úložiště klíčů přímo správci front, spusťte následující příkaz **CHGMQM** a nahraďte hodnotu *queue_manager* názvem správce front a hodnotu *password* heslem úložiště klíčů.

```
CHGMQM MQMNAME('queue_manager') SSLKEYRPWD('password')
```

Upozornění: Ujistěte se, že název a heslo správce front uzavřete do jednoduchých uvozovek, jinak produkt IBM MQ převede znaky na velká písmena.

Je-li heslo úložiště klíčů zadáno pomocí této metody, je před uložením zašifrováno pomocí systému ochrany hesla IBM MQ .

K zašifrování hesla se používá šifrovací klíč, který je znám jako počáteční klíč. Nastavte správce front tak, aby používal jedinečný počáteční klíč k bezpečné ochraně hesla. Pokud nezadáte počáteční klíč, použije se výchozí klíč.

Před nastavením hesla úložiště klíčů zkontrolujte, zda je správce front konfigurován s použitím jedinečného počátečního klíče. Počáteční klíč můžete upravit pomocí atributu **INITKEY** v příkazu **ALTER QMGR** . Příklad:

```
ALTER QMGR INITKEY('mykey')
```

Upozornění: Pokud po nastavení hesla úložiště klíčů upravíte počáteční klíč, heslo úložiště klíčů nebude zašifrováno novým počátečním klíčem. Změníte-li počáteční klíč, musíte také resetovat heslo úložiště klíčů. Jinak produkt IBM MQ nemůže dešifrovat heslo úložiště klíčů, a proto nemůže přistoupit k úložišti klíčů.

Další informace o atributu **SSLKEYRPWD** viz Parametr **SSLKEYRPWD** v **CHGMQM** příkazu.

Související pojmy

“Šifrování hesel úložiště klíčů v systému IBM i” na stránce 277
Několik komponent produktu IBM MQ potřebuje přístup k úložišti klíčů, které obsahuje digitální certifikáty nebo symetrické klíče. Úložiště klíčů je zabezpečeno heslem, protože obsahuje citlivé informace. Heslo úložiště klíčů musí být uloženo v umístění, kde jej může produkt IBM MQ číst při přístupu k úložišti klíčů. Heslo musí být také zašifrováno, aby se snížila pravděpodobnost neoprávněného přístupu k úložišti klíčů.

“Zadání hesla úložiště klíčů pro IBM MQ MQI client on IBM i” na stránce 281
Protože úložiště klíčů obsahuje citlivé informace, je zabezpečeno heslem. Chcete-li mít přístup k obsahu úložiště klíčů za účelem provádění operací TLS, musí být produkt IBM MQ schopen načíst heslo úložiště klíčů.

V 9.3.0 IBM i V 9.3.0 *Zadání hesla úložiště klíčů pro IBM MQ MQI client on IBM i*

Protože úložiště klíčů obsahuje citlivé informace, je zabezpečeno heslem. Chcete-li mít přístup k obsahu úložiště klíčů za účelem provádění operací TLS, musí být produkt IBM MQ schopen načíst heslo úložiště klíčů.

Produkt IBM MQ poskytuje čtyři mechanizmy pro dodání hesla úložiště klíčů IBM MQ MQI client:

- “Pole KeyRepoPassword modulu MQSCO ” na stránce 282
- “Proměnná prostředí MQKEYRPWD” na stránce 282
- “Atribut SSLKeyRepositoryPassword konfiguračního souboru klienta” na stránce 283
- “Soubor pro dočasné ukládání úložiště klíčů” na stránce 283

Pokud nepoužíváte soubor pro dočasné ukládání úložiště klíčů, můžete zadat heslo úložiště klíčů jako řetězec v prostém textu nebo jako řetězec, který je šifrován pomocí systému ochrany hesla IBM MQ . Další informace o metodách ochrany hesla úložiště klíčů viz “Šifrování hesel úložiště klíčů v systému IBM i” na stránce 277.

Pole KeyRepoPassword modulu MQSCO

Chcete-li zadat heslo úložiště klíčů pomocí struktury MQSCO, musíte použít kombinaci následujících tří polí řetězce proměnné:

KeyRepoPasswordLength
Délka hesla.

KeyRepoPasswordPtr
Ukazatel na umístění v paměti, které obsahuje heslo.

KeyRepoPasswordOffset
Umístění hesla v paměti reprezentované počtem bajtů od začátku struktury MQSCO.

Poznámka: Můžete dodat pouze jeden z **KeyRepoPasswordPtr** nebo **KeyRepoPasswordOffset**.

Příklad:

```
char * pwd = "passw0rd";
MQSCO  SslConnOptions = {MQSCO_DEFAULT};

SslConnOptions.KeyRepoPasswordPtr = pwd;
SslConnOptions.KeyRepoPasswordLength = (MQLONG)strlen(SslConnOptions.KeyRepoPasswordPtr);
SslConnOptions.Version = MQSCO_VERSION_6;
```

Upozornění: Zadáte-li heslo pomocí této metody, zašifrujte heslo před jeho dodáním do aplikace IBM MQ client . Další informace viz téma “Šifrování hesla úložiště klíčů” na stránce 283.

Další informace o struktuře MQCSO naleznete v tématu Volby konfigurace MQSCO-SSL/TLS.

Proměnná prostředí *MQKEYRPWD*

Pokud není klientovi dodáno heslo úložiště klíčů pomocí struktury MQSCO, můžete zadat heslo úložiště klíčů pomocí proměnné prostředí *MQKEYRPWD* . Příklad:

```
export MQKEYRPWD=passw0rd
```

, nebo

```
set MQKEYRPWD=passw0rd
```

kde *passw0rd* je vaše heslo.

Upozornění: Zadáte-li heslo pomocí této metody, před nastavením hodnoty proměnné prostředí heslo zašifrujte. Další informace viz téma “Šifrování hesla úložiště klíčů” na stránce 283.

Atribut SSLKeyRepositoryPassword konfiguračního souboru klienta

Pokud není klientovi dodáno heslo úložiště klíčů pomocí jedné z ostatních metod, můžete zadat heslo úložiště klíčů pomocí atributu **SSLKeyRepositoryPassword** v sekci **SSL** konfiguračního souboru klienta. Příklad:

```
SSL:
    SSLKeyRepositoryPassword=passw0rd
```

Upozornění: Pokud zadáte heslo pomocí této metody, zašifrujte heslo před nastavením hodnoty atributu **SSLKeyRepositoryPassword** . Další informace viz téma “Šifrování hesla úložiště klíčů” na stránce 283.

Další informace o sekci SSL konfiguračního souboru klienta viz Sekce SSL konfiguračního souboru klienta.

Soubor pro dočasné ukládání úložiště klíčů

Není-li klientovi dodáno heslo úložiště klíčů pomocí jedné z ostatních metod, produkt IBM MQ předpokládá, že soubor pro dočasné ukládání existuje ve stejném adresáři jako úložiště klíčů. Soubor pro dočasné ukládání má stejný kmenový název jako úložiště klíčů, ale má příponu `.sth` .

Soubor pro dočasné ukládání úložiště klíčů je vytvořen pomocí nástroje příkazového řádku **amqrsslc** . Chcete-li vytvořit soubor pro dočasné ukládání, spusťte následující příkaz:

```
CALL PGM(QMQM/AMQRSSLC) PARM('-s' '/Path/Of/KeyDatabase/MyKey')
```

Tento příkaz vás vyzve k zašifrování hesla. Heslo je šifrováno systémem ochrany hesla IBM MQ pomocí výchozího šifrovacího klíče, pokud není poskytnuto pomocí parametru **-sf** .

Další informace naleznete v tématech “IBM MQ Obslužný program klienta SSL (amqrsslc) pro IBM i” na stránce 291 a “Šifrování hesla úložiště klíčů” na stránce 283.

Šifrování hesla úložiště klíčů

Pokud zadáte heslo úložiště klíčů pomocí jiné metody než souboru pro dočasné ukládání, zašifrujte heslo pomocí systému ochrany hesla IBM MQ . Chcete-li heslo zašifrovat, spusťte příkaz **runmqicred** . Po zobrazení výzvy zadejte heslo úložiště klíčů. Výstupem příkazu je šifrované heslo. Zašifrované heslo lze zadat do souboru IBM MQ MQI client namísto hesla ve formátu prostého textu pomocí libovolné z popsaných metod.

K zašifrování hesla se používá šifrovací klíč, který je znám jako počáteční klíč. Při šifrování hesla použijte jedinečný počáteční klíč k bezpečné ochraně hesla. Chcete-li zadat vlastní počáteční klíč, použijte parametr **-sf** příkazu **runmqicred** . Pokud nezadáte počáteční klíč, použije se výchozí klíč.

Další informace naleznete v tématu runmqicred (ochrana hesel klienta IBM MQ).

Pokud zadáte svůj vlastní počáteční klíč, když je heslo úložiště klíčů šifrováno, a zadáte zašifrované heslo do souboru IBM MQ MQI client, musíte také zajistit, že zadáte stejný počáteční klíč do souboru IBM MQ MQI client. Další informace o tom, jak poskytnout počáteční klíč pro IBM MQ MQI client, viz “Zadání počátečního klíče pro IBM MQ MQI client on IBM i” na stránce 284.

Související pojmy

“Šifrování hesel úložiště klíčů v systému IBM i” na stránce 277
Několik komponent produktu IBM MQ potřebuje přístup k úložišti klíčů, které obsahuje digitální certifikáty nebo symetrické klíče. Úložiště klíčů je zabezpečeno heslem, protože obsahuje citlivé informace. Heslo úložiště klíčů musí být uloženo v umístění, kde jej může produkt IBM MQ číst při přístupu k úložišti klíčů. Heslo musí být také zašifrováno, aby se snížila pravděpodobnost neoprávněného přístupu k úložišti klíčů.

“Zadání hesla úložiště klíčů pro správce front v systému IBM i” na stránce 281
Protože úložiště klíčů obsahuje citlivé informace, je zabezpečeno heslem. Chcete-li mít přístup k obsahu úložiště klíčů za účelem provádění operací TLS, musí být produkt IBM MQ schopen načíst heslo úložiště klíčů.

V 9.3.0 IBM i V 9.3.0 *Zadání počátečního klíče pro IBM MQ MQI client on IBM i*

Pokud zadáte proměnné pro IBM MQ MQI client , které byly zašifrovány pomocí systému IBM MQ Password Protection System, možná budete muset zadat odpovídající počáteční klíč, který byl použit k zašifrování hodnoty.

Pokud jste při šifrování hodnoty nezadali počáteční klíč, nemusíte do parametru IBM MQ clientzadávat žádnou počáteční hodnotu klíče. Pokud jste však použili jedinečný počáteční klíč, můžete poskytnout počáteční klíč produktu IBM MQ client pomocí následujících metod:

- “Zadání počátečního klíče pomocí struktury MQCSP” na stránce 284
- “Zadání počátečního klíče pomocí proměnné prostředí MQS_MQI_KEYFILE” na stránce 284
- “Zadání počátečního klíče pomocí konfiguračního souboru klienta” na stránce 284

Zadání počátečního klíče pomocí struktury MQCSP

Chcete-li zadat počáteční klíč pomocí struktury MQCSP, musíte použít kombinaci následujících tří polí řetězce proměnné:

InitialKeyLength
Délka počátečního klíče

InitialKeyPtr
Ukazatel na umístění v paměti obsahující počáteční klíč

InitialKeyOffset
Umístění počátečního klíče v paměti reprezentované počtem bajtů od začátku struktury MQCSP.

Poznámka: Můžete dodat pouze jeden z **InitialKeyPtr** nebo **InitialKeyOffset**.

Příklad:

```
char * initialKey = "myInitialKey";
MQCSP  cspOptions = {MQCSP_DEFAULT};


cspOptions.InitialKeyPtr = initialKey;
cspOptions.InitialKeyLength = (MQLONG)strlen(cspOptions.InitialKeyPtr);
cspOptions.Version = MQCSP_VERSION_2;
```

Zadání počátečního klíče pomocí proměnné prostředí MQS_MQI_KEYFILE

Není-li klientovi pomocí struktury MQCSP dodán počáteční klíč, produkt IBM MQ zkontroluje proměnnou prostředí *MQS_MQI_KEYFILE* . Tuto proměnnou prostředí byste měli nastavit na umístění souboru obsahujícího jeden řádek textu, který se skládá z počátečního klíče, který chcete použít.

Pokud například v kořenovém adresáři existuje soubor s názvem `mykey.key` a obsahuje počáteční klíč, měli byste nastavit proměnnou prostředí takto:

```
export MQS_MQI_KEYFILE=/mykey.key
```

, nebo

```
set MQS_MQI_KEYFILE=C:\mykey.key
```

Zadání počátečního klíče pomocí konfiguračního souboru klienta

Pokud není počáteční klíč dodán klientovi pomocí předchozího mechanizmu, IBM MQ zkontroluje atribut **MQIInitialKeyFile** sekce zabezpečení souboru `mqclient.ini` . Tento atribut byste měli nastavit na umístění souboru obsahujícího jeden řádek textu, který se skládá z počátečního klíče, který chcete použít.

Pokud například v kořenovém adresáři existuje soubor s názvem `mykey.key` a obsahuje počáteční klíč, měl by konfigurační soubor klienta obsahovat následující:

```
Security:
    MQIInitialKeyFile=/mykey.key
```

Související pojmy

“Šifrování hesel úložiště klíčů v systému IBM i” na stránce 277
Několik komponent produktu IBM MQ potřebuje přístup k úložišti klíčů, které obsahuje digitální certifikáty nebo symetrické klíče. Úložiště klíčů je zabezpečeno heslem, protože obsahuje citlivé informace. Heslo úložiště klíčů musí být uloženo v umístění, kde jej může produkt IBM MQ číst při přístupu k úložišti klíčů. Heslo musí být také zašifrováno, aby se snížila pravděpodobnost neoprávněného přístupu k úložišti klíčů.

“Práce se zabezpečením SSL/TLS v systému IBM i” na stránce 276
Tato kolekce témat poskytuje pokyny pro jednotlivé úlohy pracující s protokolem TLS (Transport Layer Security) v produktu IBM MQ for IBM i.

Vytvoření certifikační autority a certifikátu pro testování na systému IBM i

Tento postup slouží k vytvoření certifikátu lokálního CA pro podepisování žádostí o certifikáty a k vytvoření a instalaci certifikátu CA.

Než začnete

Pokyny v tomto tématu předpokládají, že lokální certifikační autorita (CA) neexistuje. Pokud lokální CA existuje, přejděte do adresáře “Vyžádání certifikátu serveru v systému IBM i” na stránce 286.

Informace o této úloze

Certifikáty CA, které jsou poskytnuty při instalaci TLS, jsou podepsány vydávající certifikační autoritou. V systému IBM i můžete generovat lokální certifikační autoritu, která může podepisovat certifikáty serveru pro testování komunikací TLS ve vašem systému. Chcete-li vytvořit certifikát lokální CA, postupujte ve webovém prohlížeči takto:

Postup

1. Přistupte k rozhraní DCM, jak je popsáno v tématu “Přístup k produktu DCM” na stránce 276.
2. V navigačním panelu klepněte na volbu **Vytvořit certifikační autoritu**.

   V rámci úlohy se zobrazí stránka Vytvořit certifikační autoritu.
3. Zadejte heslo do pole **Heslo úložiště certifikátů** a zadejte je znovu do pole **Potvrzení hesla** .
4. Zadejte název do pole **Název certifikační autority (CA)** , například `TLS Test Certificate Authority`.
5. Zadejte odpovídající hodnoty do polí **Obecný název** a **Organizace** a vyberte zemi. Pro zbývající volitelná pole zadejte požadované hodnoty.
6. Do pole **Období platnosti** zadejte období platnosti pro lokální CA.

   Výchozí hodnota je 1095 dnů.
7. Klepněte na tlačítko **Pokračovat**.

   CA se vytvoří a DCM vytvoří úložiště certifikátů a certifikát CA pro vašeho lokálního CA.
8. Klepněte na volbu **Instalovat certifikát**.

   Zobrazí se dialogové okno Správce stahování.
9. Zadejte úplnou cestu k dočasnému souboru, do kterého chcete uložit certifikát CA, a klepněte na tlačítko **Uložit**.
10. Po dokončení stahování klepněte na tlačítko **Otevřít**.

    Zobrazí se okno Certifikát.
11. Klepněte na volbu **Instalovat certifikát**.

    Zobrazí se průvodce importem certifikátu.

12. Klepněte na tlačítko **Další**.
13. Vyberte volbu **Automaticky vybrat úložiště certifikátů na základě typu certifikátu** a klepněte na tlačítko **Další**.
14. Klepněte na tlačítko **Dokončit**.

    Zobrazí se potvrzovací okno.
15. Klepněte na tlačítko **OK**.
16. V okně Certifikát klepněte na tlačítko **OK**.
17. Klepněte na tlačítko **Pokračovat**.

    V rámci úlohy se zobrazí stránka Zásada certifikační autority.
18. V poli **Povolit vytváření uživatelských certifikátů** vyberte volbu **Ano**.
19. Do pole **Období platnosti** zadejte období platnosti certifikátů vydaných lokální CA.

    Výchozí hodnota je 365 dní.
20. Klepněte na tlačítko **Pokračovat**.

    V rámci úlohy se zobrazí stránka Vytvořit certifikát v novém úložišti certifikátů.
21. Zkontrolujte, zda není vybrána žádná z aplikací.
22. Klepnutím na tlačítko **Pokračovat** dokončete nastavení lokálního CA.

Jak pokračovat dále

Potřebujete-li obnovit existující certifikát, přečtěte si téma Obnovení existujícího certifikátu v dokumentaci k produktu IBM i .

Vyžádání certifikátu serveru v systému IBM i

Digitální certifikáty chrání před zosobněním, což potvrzuje, že veřejný klíč patří určené entitě. Nový certifikát serveru lze požadovat od certifikační autority pomocí produktu DCM (Digital Certificate Manager).

Informace o této úloze

Ve webovém prohlížeči proveďte následující kroky:

Postup

1. Přistupte k rozhraní DCM, jak je popsáno v tématu “Přístup k produktu DCM” na stránce 276.
2. V navigačním panelu klepněte na volbu **Vybrat úložiště certifikátů**.

   V rámci úlohy se zobrazí stránka Vybrat úložiště certifikátů.
3. Vyberte úložiště certifikátů, které chcete použít, a klepněte na tlačítko **Pokračovat**.
4. Volitelné: Pokud jste v kroku 3 vybrali volbu ***SYSTEM** , zadejte heslo systémového úložiště a klepněte na tlačítko **Pokračovat**.
5. Volitelné: Pokud jste v kroku 3 vybrali volbu **Jiné systémové úložiště certifikátů** , do pole **Cesta a název souboru úložiště certifikátů** zadejte cestu IFS a název souboru, který jste nastavili při vytváření úložiště certifikátů. Zadejte také heslo do pole **Heslo úložiště certifikátů** . Pak klepněte na tlačítko **Pokračovat**
6. V navigačním panelu klepněte na volbu **Vytvořit certifikát**.
7. V rámci úlohy vyberte přepínač **Certifikát serveru nebo klienta** a klepněte na tlačítko **Pokračovat**.

   V rámci úlohy se zobrazí stránka Vybrat certifikační autoritu (CA).
8. Máte-li na pracovní stanici lokálního CA, vyberte buď lokálního CA, nebo komerčního CA pro podepsání certifikátu. Vyberte přepínač pro požadovanou certifikační autoritu a klepněte na tlačítko **Pokračovat**.

   V rámci úlohy se zobrazí stránka Vytvořit certifikát.
9. Volitelné: V případě správce front zadejte do pole **Popisek certifikátu** popisek certifikátu.

Popisek je buď hodnota atributu **CERTLABL** , je-li nastaven, nebo výchozí hodnota `ibmwebspheremq` s připojeným názvem správce front, vše malými písmeny. Podrobnosti viz Popisky digitálních certifikátů .

Například pro správce front QM1zadejte `ibmwebspheremqqm1` , chcete-li použít výchozí hodnotu.

10. Volitelné: V případě položky IBM MQ MQI clientzadejte do pole **Popisek certifikátu** hodnotu `ibmwebspheremq` následovanou vaším přihlašovacím ID uživatele složeným na malá písmena. Zadejte například `ibmwebspheremqmyuserID`
11. Zadejte odpovídající hodnoty do polí **Obecný název** a **Organizace** a vyberte zemi. Pro zbývající volitelná pole zadejte požadované hodnoty.

Výsledky

Pokud jste pro podepsání certifikátu vybrali komerční CA, produkt DCM vytvoří žádost o certifikát ve formátu PEM (Privacy-Enhanced Mail). Předejte požadavek vybrané certifikační autoritě.

Pokud jste pro podepsání certifikátu vybrali lokálního CA, produkt DCM vás informuje, že certifikát byl vytvořen v úložišti certifikátů a lze jej použít.

Vyžádání certifikátu serveru pro IBM Správce klíčů na IBM i

Postupujte takto, chcete-li vytvořit certifikát podepsaný lokální certifikační autoritou (CA) nebo požádat o certifikát serveru podepsaný komerční certifikační autoritou pro import do obslužného programu IBM Správa klíčů (iKeyman).

Informace o této úloze

Uživatelský certifikát musí být použit, když produkt DCM (Digital Certificate Manager) slouží jako správce certifikátů pro produkt IBM MQ na více platformách. Pro osobní certifikáty distribuované na jiné platformy a pro import do obslužného programu iKeyman proveďte ve webovém prohlížeči následující kroky:

Postup

1. Přistupte k rozhraní DCM, jak je popsáno v tématu “Přístup k produktu DCM” na stránce 276.
2. V **navigačním** podokně klepněte na volbu **Vytvořit certifikát**.

   V rámci úlohy se zobrazí stránka **Vytvořit certifikát** .
3. Na panelu **Vytvořit certifikát** vyberte přepínač **Uživatelský certifikát** a klepněte na tlačítko **Pokračovat**.

   Zobrazí se stránka **Vytvořit uživatelský certifikát** .
4. Na panelu **Vytvořit uživatelský certifikát** vyplňte požadovaná pole v části Informace o certifikátu pro **Název organizace**, **Stát** nebo **kraj**, **Země** nebo **oblast**. Volitelně zadejte hodnoty do polí **Organizační jednotka** a **Lokalita** nebo **město** . Klepněte na tlačítko **Pokračovat**.

   Obecné jméno je automaticky nastaveno na ID uživatele, pod kterým jste přihlášeni k systému iSeries .
5. Na dalším panelu **Vytvořit uživatelský certifikát** klepněte na volbu **Instalovat certifikát** a klepněte na tlačítko **Pokračovat**.

   Zobrazí se zpráva s informací `Váš osobní certifikát byl nainstalován. Měli byste uchovat záložní kopii tohoto certifikátu.`
6. Klepněte na tlačítko **OK**.
7. V závislosti na internetovém prohlížeči, který jste použili pro přístup k produktu DCM, postupujte takto:
   a) Pro položku Microsoft Edge zvolte: **Nástroje > Možnosti Internetu > karta Obsah > tlačítko Certifikáty > Osobní karta >**. Vyberte certifikát a klepněte na tlačítko **Exportovat**.
   b) V případě prohlížeče Mozilla Firefox zvolte: **Nástroje > Volby > Rozšířené > karta Šifrování > tlačítko Zobrazit certifikáty > karta Certifikáty >**. Vyberte certifikát a klepněte na tlačítko **Zálohovat**. Vyberte cestu a název souboru a klepněte na tlačítko **OK**.
8. Přeneste exportovaný certifikát na vzdálený systém pomocí protokolu FTP v binárním formátu.
9. Přidejte exportovaný certifikát z kroku 7 do obslužného programu iKeyman v databázi klíčů.

a) Pokud byl certifikát uložen pomocí produktu Microsoft Edge, postupujte podle pokynů popsaných v části Import ze souboru Microsoft `.pfx` .

b) Pokud byl certifikát uložen pomocí prohlížeče Mozilla Firefox, postupujte podle pokynů popsaných v tématu Import osobního certifikátu do úložiště klíčů.

Během importu se ujistěte, že název popisku osobního certifikátu a certifikátu podepsaného byly změněny na to, co produkt IBM MQ očekává. Popisek musí být buď hodnota atributu IBM MQ **CERTLABL** , je-li nastaven, nebo výchozí hodnota `ibmwebspheremq` s připojeným názvem správce front, vše malými písmeny. Podrobnosti viz Popisky digitálních certifikátů .

Přidání certifikátů serveru do úložiště klíčů v systému IBM i

Chcete-li přidat požadovaný certifikát do úložiště klíčů, postupujte takto.

Informace o této úloze

Poté, co vám certifikační autorita odešle nový certifikát serveru, přidejte jej do úložiště certifikátů, ze kterého jste vygenerovali požadavek. Pokud certifikační autorita odešle certifikát jako součást e-mailové zprávy, zkopírujte certifikát do samostatného souboru.

Poznámka:

- Tento postup není nutné provádět, pokud je certifikát serveru podepsán lokální CA.
- Před importem certifikátu serveru ve formátu PKCS #12 do produktu DCM musíte nejprve importovat odpovídající certifikát CA.

Chcete-li přijmout certifikát serveru do úložiště certifikátů správce front, postupujte takto:

Postup

1. Přistupte k rozhraní DCM, jak je popsáno v tématu “Přístup k produktu DCM” na stránce 276.
2. V kategorii úloh **Spravovat certifikáty** v navigačním panelu klepněte na volbu **Importovat certifikát**.

   V rámci úlohy se zobrazí stránka Importovat certifikát.
3. Vyberte přepínač pro typ certifikátu a klepněte na tlačítko **Pokračovat**.

   V rámci úlohy se zobrazí stránka Importovat certifikát serveru nebo klienta nebo stránka Importovat certifikát certifikační autority (CA).
4. Do pole **Import souboru** zadejte název souboru certifikátu, který chcete importovat, a klepněte na tlačítko **Pokračovat**.

   Produkt DCM automaticky určuje formát souboru.
5. Pokud je certifikát certifikátem **Server nebo klient** , zadejte heslo do rámce úlohy a klepněte na tlačítko **Pokračovat**.

   Produkt DCM vás informuje, že certifikát byl importován.

Export certifikátu z úložiště klíčů na systému IBM i

Export certifikátu exportuje veřejný i soukromý klíč. Tato opatření by měla být přijata s mimořádnou opatrností, protože předání soukromého klíče by zcela ohrozilo vaši bezpečnost.

Než začnete

Sdílíte-li certifikát uživatele s jiným uživatelem, vyměňujete si veřejné klíče. Tento proces je popsán v části **Úloha 5. Sdílení certifikátů** v části Sdílení certifikátů “Stručná úvodní příručka pro AMS on AIX and Linux” na stránce 628. Při exportu certifikátu, jak je popsáno zde, exportujete veřejný i soukromý klíč. Tato opatření by měla být přijata s mimořádnou opatrností, protože předání soukromého klíče by zcela ohrozilo vaši bezpečnost.

Informace o této úloze

Na počítači, ze kterého chcete exportovat certifikát, postupujte takto:

Postup

1. Přistupte k rozhraní DCM, jak je popsáno v tématu “Přístup k produktu DCM” na stránce 276.
2. V navigačním panelu klepněte na volbu **Vybrat úložiště certifikátů**.

   V rámci úlohy se zobrazí stránka Vybrat úložiště certifikátů.
3. Vyberte úložiště certifikátů, které chcete použít, a klepněte na tlačítko **Pokračovat**.
4. Volitelné: Pokud jste v kroku 3 vybrali volbu ***SYSTEM** , zadejte heslo systémového úložiště a klepněte na tlačítko **Pokračovat**.
5. Volitelné: Pokud jste v kroku 3 vybrali volbu **Jiné systémové úložiště certifikátů** , do pole **Cesta a název souboru úložiště certifikátů** zadejte cestu IFS a název souboru, který jste nastavili při vytváření úložiště certifikátů, a zadejte heslo do pole **Heslo úložiště certifikátů** . Pak klepněte na tlačítko **Pokračovat**
6. V kategorii úloh **Spravovat certifikáty** v navigačním panelu klepněte na volbu **Exportovat certifikát**.

   V rámci úlohy se zobrazí stránka Exportovat certifikát.
7. Vyberte přepínač pro typ certifikátu a klepněte na tlačítko **Pokračovat**.

   V rámci úlohy se zobrazí stránka Exportovat certifikát serveru nebo klienta nebo stránka Exportovat certifikát certifikační autority (CA).
8. Vyberte certifikát, který chcete exportovat.
9. Výběrem přepínače určete, zda chcete exportovat certifikát do souboru nebo přímo do jiného úložiště certifikátů.
10. Pokud jste vybrali export certifikátu serveru nebo klienta do souboru, zadejte následující informace:
    - Cesta a název souboru umístění, kam chcete uložit exportovaný certifikát.
    - V případě osobního certifikátu se jedná o heslo, které se používá k zašifrování exportovaného certifikátu a cílového vydání. U certifikátů CA nemusíte zadávat heslo.
11. Pokud jste se rozhodli exportovat certifikát přímo do jiného úložiště certifikátů, zadejte cílové úložiště certifikátů a jeho heslo.
12. Klepněte na tlačítko **Pokračovat**.

Import certifikátu do úložiště klíčů v systému IBM i

Chcete-li importovat certifikát, postupujte podle této procedury.

Než začnete

Před importem osobního certifikátu ve formátu PKCS #12 do produktu DCM musíte nejprve importovat odpovídající certifikát CA.

Informace o této úloze

Proveďte tyto kroky na počítači, do kterého chcete importovat certifikát.

Postup

1. Přistupte k rozhraní DCM, jak je popsáno v tématu “Přístup k produktu DCM” na stránce 276.
2. V navigačním panelu klepněte na volbu **Vybrat úložiště certifikátů**.

   V rámci úlohy se zobrazí stránka Vybrat úložiště certifikátů.
3. Vyberte úložiště certifikátů, které chcete použít, a klepněte na tlačítko **Pokračovat**.
4. Volitelné: Pokud jste v kroku 3 vybrali volbu ***SYSTEM** , zadejte heslo systémového úložiště a klepněte na tlačítko **Pokračovat**.
5. Volitelné: Pokud jste v kroku 3 vybrali volbu **Jiné systémové úložiště certifikátů** , do pole **Cesta a název souboru úložiště certifikátů** zadejte cestu IFS a název souboru, který jste nastavili při vytváření úložiště certifikátů, a zadejte heslo do pole **Heslo úložiště certifikátů** . Pak klepněte na tlačítko **Pokračovat**
6. V kategorii úloh **Spravovat certifikáty** v navigačním panelu klepněte na volbu **Importovat certifikát**.

V rámci úlohy se zobrazí stránka Importovat certifikát.

7. Vyberte přepínač pro typ certifikátu a klepněte na tlačítko **Pokračovat**.

   V rámci úlohy se zobrazí stránka Importovat certifikát serveru nebo klienta nebo stránka Importovat certifikát certifikační autority (CA).

8. Do pole **Import souboru** zadejte název souboru certifikátu, který chcete importovat, a klepněte na tlačítko **Pokračovat**.

   Produkt DCM automaticky určuje formát souboru.

9. Pokud je certifikát certifikátem **Server nebo klient** , zadejte heslo do rámce úlohy a klepněte na tlačítko **Pokračovat**. Produkt DCM vás informuje, že certifikát byl importován.

Odebrání certifikátů v adresáři IBM i

Tento postup slouží k odebrání osobních certifikátů.

Postup

1. Přistupte k rozhraní DCM, jak je popsáno v tématu “Přístup k produktu DCM” na stránce 276.
2. V navigačním panelu klepněte na volbu **Vybrat úložiště certifikátů**.

   V rámci úlohy se zobrazí stránka Vybrat úložiště certifikátů.

3. Označte zaškrtávací políčko **Jiná systémová paměť certifikátů** a klepněte na tlačítko **Pokračovat**.

   Zobrazí se stránka Úložiště certifikátů a heslo.

4. Do pole **Cesta a název souboru úložiště certifikátů** zadejte cestu IFS a název souboru, který jste nastavili při vytváření úložiště certifikátů.
5. Zadejte heslo do pole **Heslo úložiště certifikátů** . Klepněte na tlačítko **Pokračovat**.

   V rámci úlohy se zobrazí stránka Aktuální úložiště certifikátů.

6. V kategorii úloh **Spravovat certifikáty** v navigačním panelu klepněte na volbu **Odstranit certifikát**.

   V rámci úlohy se zobrazí stránka Potvrdit odstranění certifikátu.

7. Vyberte certifikát, který chcete odstranit. Klepněte na tlačítko **Odstranit**.
8. Klepnutím na tlačítko **Ano** potvrďte, že chcete odstranit certifikát. Jinak klepněte na volbu **Ne**.

   Produkt DCM vás informuje, zda certifikát odstranil.

*Použití úložiště certifikátů *SYSTEM pro jednosměrné ověření v systému IBM i*

Chcete-li nastavit jednosměrné ověření, postupujte podle těchto pokynů.

Než začnete

- Vytvořte správce front, kanály a přenosové fronty.
- Vytvořte certifikát serveru nebo klienta ve správci front serveru.
- Přeneste certifikát CA do správce front klienta a naimportujte jej do úložiště klíčů.
- Spusťte modul listener na správci front serveru a klienta.

Informace o této úloze

Chcete-li použít jednosměrné ověření a použít počítač se systémem IBM i jako serverem TLS, nastavte parametr SSLKEYR (SSL Key Repository) na hodnotu *SYSTEM. Toto nastavení registruje správce front IBM MQ jako aplikaci. Poté můžete správci front přiřadit certifikát, který umožní jednosměrné ověřování.

Můžete také použít soukromá úložiště klíčů k implementaci jednosměrného ověření vytvořením fiktivního certifikátu pro správce front klienta v úložišti klíčů.

Postup

1. Na správci front serveru a klienta proveďte následující kroky:

a) Změňte správce front tak, aby nastavil parametr SSLKEYR, zadáním příkazu `CHGMQM MQMNAME(SSL) SSLKEYR(*SYSTEM)`.

b) Zadáním příkazu `CHGMQM MQMNAME(SSL) SSLKEYRPWD('xxxxxxx')` heslo pro výchozí úložiště klíčů schovte.

Heslo musí být v apostrofech.

c) Upravte kanály tak, aby měly správnou specifikaci CipherSpec v parametru SSLCIPHER.

d) Obnovte zabezpečení TLS zadáním příkazu `RFRMQMAUT QMNAME(QMGRNAME) TYPE(*SSL)`.

2. Přiřaďte certifikát správci front serveru pomocí produktu DCM takto:

a) Přistupte k rozhraní DCM, jak je popsáno v tématu "Přístup k produktu DCM" na stránce 276.

b) V navigačním panelu klepněte na volbu **Vybrat úložiště certifikátů**.

V rámci úlohy se zobrazí stránka Vybrat úložiště certifikátů.

c) Vyberte úložiště certifikátů *SYSTEM a klepněte na tlačítko **Pokračovat**.

d) V levém panelu rozbalte položku **Spravovat aplikace**.

e) Výběrem definice **Zobrazit aplikaci** zkontrolujte, zda byl správce front registrován jako aplikace.

V tabulce je uvedeno SSL `(WMQ)`.

f) Vyberte volbu **Aktualizovat přiřazení certifikátu**.

g) Vyberte **Server** a klepněte na tlačítko **Pokračovat**.

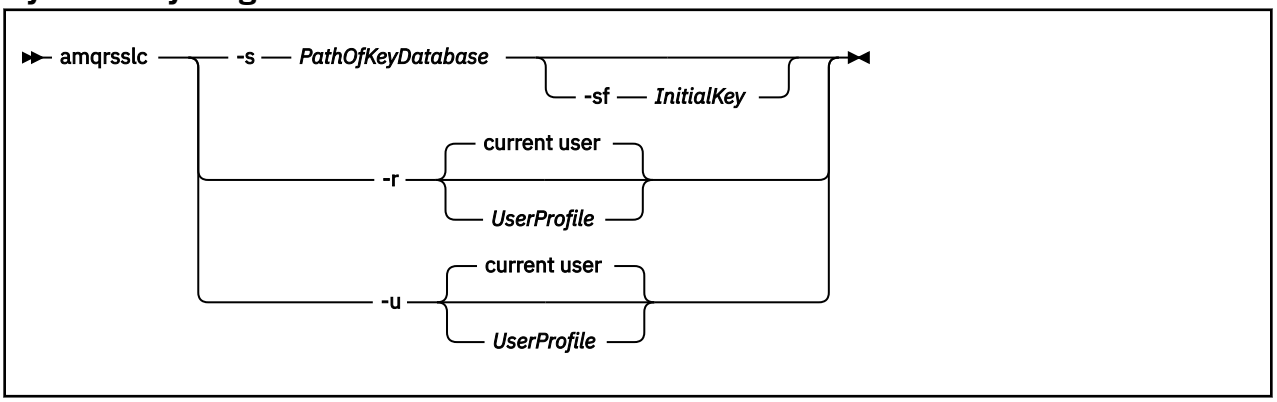
h) Vyberte QMGRNAME (WMQ) a klepněte na volbu **Aktualizovat přiřazení certifikátu**.

i) Vyberte certifikát a klepněte na volbu **Přiřadit nový certifikát**. Otevře se okno s informací, že certifikát byl přiřazen k aplikaci.

IBM MQ Obslužný program klienta SSL (amqrsslc) pro IBM i

Obslužný program IBM MQ SSL Client (amqrsslc) for IBM i používá systém IBM MQ MQI client na systémech IBM i k registraci nebo zrušení registrace profilu uživatele klienta nebo k uložení hesla úložiště certifikátů. Obslužný program může spustit pouze uživatel se speciálním oprávněním *ALLOBJ nebo člen QMQMADM, který má volby pro vytváření nebo odstraňování registrací aplikací v produktu DCM (Digital Certificate Manager).

Syntaktický diagram



Registrovat profil uživatele klienta

Pokud produkt IBM MQ MQI client používá úložiště certifikátů *SYSTEM, musíte zaregistrovat profil uživatele klienta (přihlášeného uživatele) pro použití jako aplikace s produktem Digital Certificate Manager (DCM).

Chcete-li zaregistrovat profil uživatele klienta, spusťte program **amqrsslc** s volbou `-r` s volbou *UserProfile*. Profil uživatele použitý při volání **amqrsslc** musí mít oprávnění *USE. Zadáním hodnoty *UserProfile* s volbou `-r` zaregistruje profil uživatele *UserProfile* jako serverovou aplikaci s jedinečným popiskem aplikace QIBM_WEBSPHERE_MQ_*UserProfile* a popiskem s popisem *UserProfile* (WMQ). Tato

serverová aplikace se pak zobrazí v produktu DCM a můžete této aplikaci přiřadit libovolný serverový nebo klientský certifikát v systémovém úložišti.

Poznámka: Není-li profil uživatele uveden s volbou `-r` , je registrován profil uživatele, který spustil nástroj **amqrsslc** .

Následující kód používá produkt **amqrsslc** k registraci profilu uživatele. V prvním příkladu je uvedený profil uživatele registrován; ve druhém je to profil přihlášeného uživatele:

```
CALL PGM(QMQM/AMQRSSLC) PARM('-r' UserProfile)
CALL PGM(QMQM/AMQRSSLC) PARM('-r')
```

Zrušit registraci profilu uživatele klienta

Chcete-li zrušit registraci profilu klienta, spusťte program **amqrsslc** s volbou `-u` s volbou *UserProfile*. Profil uživatele použitý při volání **amqrsslc** musí mít oprávnění *USE. Zadáním příkazu *UserProfile* s volbou `-u` zrušíte registraci *UserProfile* s popiskem QIBM_WEBSPHERE_MQ_*UserProfile* z produktu DCM.

Poznámka: Pokud není profil uživatele uveden s volbou `-u` , pak je profil uživatele, který spustil nástroj **amqrsslc** , neregistrovaný.

Následující kód používá produkt **amqrsslc** ke zrušení registrace profilu uživatele. V prvním příkladu je uvedený profil uživatele neregistrovaný; ve druhém je to profil přihlášeného uživatele:

```
CALL PGM(QMQM/AMQRSSLC) PARM('-u' UserProfile)
CALL PGM(QMQM/AMQRSSLC) PARM('-u')
```

Uložit heslo úložiště certifikátů

Pokud produkt IBM MQ MQI client nepoužívá úložiště certifikátů *SYSTEM a používá jiné úložiště certifikátů (to znamená, že MQSSLKEYR je nastaveno na jinou hodnotu než *SYSTEM), pak heslo databáze klíčů může být uloženo tak, aby nemuselo být zadáno aplikací klienta při spuštění produktu.

Použijte volbu `-s` k uložení hesla databáze klíčů. V 9.3.0 Zadejte úplnou cestu a název databáze klíčů. Není-li přípona souboru dodána, předpokládá se, že je `.kdb`.

V následujícím kódu je úplný název souboru úložiště certifikátů `/Path/Of/KeyDatabase/MyKey.kdb`:

```
CALL PGM(QMQM/AMQRSSLC) PARM('-s' '/Path/Of/KeyDatabase/MyKey')
```

Spuštění tohoto kódu má za následek požadavek na heslo této databáze klíčů. Toto heslo je uloženo v souboru se stejným názvem jako databáze klíčů s příponou `.sth` .

V 9.3.0 Dále lze zadat počáteční klíč k zašifrování hesla. Počáteční klíč by měl být uložen v souboru jako jeden řádek textu a pak je umístění tohoto souboru dodáno programu prostřednictvím příznaku **-sf** . Není-li zadán žádný počáteční soubor s klíči, použije se k zašifrování hesla výchozí klíč.

Soubor pro dočasné ukládání je uložen ve stejné cestě jako databáze klíčů. Příklad kódu vygeneruje soubor pro dočasné ukládání `/Path/Of/KeyDatabase/MyKey.sth`.

QMQM je vlastníkem uživatele a QMQMADM je vlastníkem skupiny pro tento soubor. QMQM a QMQMADM mají oprávnění ke čtení, zápisu a jiné profily mají pouze oprávnění ke čtení.

Když změny certifikátů nebo úložiště certifikátů vstoupí v platnost v systému IBM i

Změníte-li certifikáty v úložišti certifikátů nebo umístění úložiště certifikátů, změny se projeví v závislosti na typu kanálu a způsobu spuštění kanálu.

Změny certifikátů v úložišti certifikátů a v atributu úložiště klíčů se projeví v následujících situacích:

- Když nový proces odchozího jednoho kanálu nejprve spustí kanál TLS.

- Když nový příchozí proces TCP/IP s jedním kanálem nejprve obdrží požadavek na spuštění kanálu TLS.
- Při zadání příkazu MQSC REFRESH SECURITY TYPE (SSL) pro aktualizaci prostředí IBM MQ TLS.
- V případě procesů aplikace klienta při zavření posledního připojení TLS v procesu. Další připojení TLS vyzvedne změny certifikátu.
- U kanálů, které jsou spuštěny jako podprocesy procesu sdružování procesů (amqrmppa), při spuštění nebo restartování procesu sdružování procesů a při prvním spuštění kanálu TLS. Pokud již proces sdružování procesů spustil kanál TLS a chcete, aby se změna okamžitě stala účinnou, spusťte příkaz MQSC REFRESH SECURITY TYPE (SSL).
- Pro kanály, které jsou spuštěny jako podprocesy inicializátoru kanálu, platí, že když je inicializátor kanálu spuštěn nebo restartován a nejprve je spuštěn kanál TLS. Pokud již proces inicializátoru kanálu spustil kanál TLS a chcete změnu provést okamžitě, spusťte příkaz MQSC REFRESH SECURITY TYPE (SSL).
- Pro kanály, které jsou spuštěny jako podprocesy modulu listener TCP/IP, platí, že když je modul listener spuštěn nebo restartován a nejprve obdrží požadavek na spuštění kanálu TLS. Pokud již modul listener spustil kanál TLS a chcete změnu provést okamžitě, spusťte příkaz MQSC REFRESH SECURITY TYPE (SSL).

Konfigurace šifrovacího hardwaru v systému IBM i

Pomocí této procedury nakonfigurujete šifrovací koprocesor na systému IBM i

Než začnete

Ujistěte se, že váš profil uživatele má speciální oprávnění *ALLOBJ a *SECADM, abyste mohli konfigurovat hardware koprocesoru.

Postup

1. Přejděte na `http://`*`machine`*`.domain:2001` nebo `https://`*`machine`*`.domain:2010`, kde *počítač* je název vašeho počítače.

   Zobrazí se dialogové okno požadující jméno uživatele a heslo.
2. Zadejte platný profil uživatele a heslo produktu IBM i .
3. Přejděte na Kryptografie a postupujte podle příslušných odkazů pro další informace.

Jak pokračovat dále

Další specifické informace o konfiguraci šifrovacího koprocesoru 4767 Cryptographic Coprocessornaleznete v tématu 4767 Cryptographic Coprocessor.

ALW Práce se zabezpečením SSL/TLS v systému AIX, Linux, and Windows

V systémech AIX, Linux, and Windows je podpora TLS (Transport Layer Security) instalována spolu s produktem IBM MQ.

Podrobnější informace o zásadách ověřování certifikátů naleznete v tématu Ověření platnosti certifikátu a návrh zásad důvěryhodnosti.

ALW *Použití příkazu runmqckm, runmqakm a strmqikm ke správě digitálních certifikátů*

V systémech AIX, Linux, and Windows spravujte klíče a digitální certifikáty pomocí konzoly **strmqikm** (iKeyman). Grafické rozhraní nebo z příkazového řádku pomocí **runmqckm** (iKeycmd) nebo **runmqakm** (GSKCapiCmd).

Poznámka: Deprecated V 9.3.4 Podpora úložiště klíčů CMS pro aplikace IBM MQ Java , AMQP a MQTT je zamítnuta z IBM MQ 9.3.4. Pokud používáte úložiště klíčů CMS s aplikacemi IBM MQ Java ,

AMQP a MQTT, měli byste migrovat na podporu úložiště klíčů PKCS#12 uvolněnou v produktu IBM MQ 9.3.0.

Nástroje **runmqckm**, **strmqikm**, **mqiptKeycmd** a **mqiptKeyman** jsou také zamítnuty. Příkaz **runmqakm** z prostředí IBM MQ a příkaz **keytool** z prostředí JRE jsou k dispozici jako alternativy.

Upozornění: Příkazy **runmqckm** i **strmqikm** spoléhají na prostředí JRE (IBM MQ Java Runtime Environment). V systému IBM MQ 9.1, není-li prostředí JRE nainstalováno, obdržíte zprávu AMQ9183.

- Linux AIX Pro systémy **AIX and Linux** :
  - Použijte příkaz **strmqikm** (iKeyman) ke spuštění grafického rozhraní iKeyman .
  - Použijte příkaz **runmqckm** k provedení úloh s rozhraním příkazového řádku.
  - Pomocí příkazu **runmqakm** (GSKCapiCmd) můžete provádět úlohy s rozhraním příkazového řádku runmqakm. Syntaxe příkazu pro **runmqakm** je stejná jako syntaxe pro **runmqckm**.

    Potřebujete-li spravovat certifikáty TLS způsobem, který vyhovuje standardu FIPS, použijte příkaz **runmqakm** namísto příkazů **runmqckm** nebo **strmqikm** .

  Úplný popis rozhraní příkazového řádku pro příkazy **runmqckm** a **runmqakm** naleznete v tématu Správa klíčů a certifikátů .

  Používáte-li certifikáty nebo klíče uložené na šifrovacím hardwaru PKCS #11 , mějte na paměti, že **runmqckm** a iKeyman jsou 64bitové programy. Externí moduly vyžadované podporou PKCS #11 se načtou do 64bitového procesu, a proto musíte mít pro administraci na šifrovacím hardwaru nainstalovanou 64bitovou knihovnu PKCS #11. 32bitové platformy Windows a Linux x86 jsou jedinými výjimkami, protože programy iKeyman a **runmqckm** jsou na těchto platformách 32bitové.

  Další informace viz IBM Global Security Kit (GSKit): PKCS#11 a IBM MQ Režim adresování JRE .

  Než spustíte příkaz **strmqikm** ke spuštění grafického rozhraní iKeyman , ujistěte se, že pracujete na počítači, který je schopen spustit systém X Window, a že provedete následující:
  - Nastavte proměnnou prostředí DISPLAY, například:

    ```
    export DISPLAY=mypc:0
    ```
  - Ujistěte se, že proměnná prostředí PATH obsahuje **/usr/bin** a **/bin**. To je také vyžadováno pro příkazy **runmqckm** a **runmqakm** . Příklad:

    ```
    export PATH=$PATH:/usr/bin:/bin
    ```
- Windows Pro systémy **Windows** :
  - Použijte příkaz **strmqikm** ke spuštění grafického rozhraní iKeyman .
  - Použijte příkaz **runmqckm** k provedení úloh s rozhraním příkazového řádku.

    Potřebujete-li spravovat certifikáty TLS způsobem, který vyhovuje standardu FIPS, použijte příkaz **runmqakm** namísto příkazů **runmqckm** nebo **strmqikm** .
  - Použijte příkaz **runmqakm -keydb** s volbou *stashpw* nebo *stash* .

    Při použití příkazu **runmqakm -keydb** tímto způsobem například:

    ```
    runmqakm -keydb -create -db key.kdb -pw secretpwd -stash
    ```

    výsledný soubor `.sth` nemá pro skupinu `mqm` povoleno oprávnění ke čtení.

    Soubor může číst pouze tvůrce. Po vytvoření souboru pro dočasné ukládání pomocí příkazu **runmqakm** zkontrolujte oprávnění k souboru a udělte oprávnění servisnímu účtu, na kterém je spuštěn správce front, nebo skupině, například lokální `mqm`.

ALW Chcete-li požadovat trasování TLS v systémech AIX, Linux, and Windows , viz strmqtrc.

Související odkazy

“příkazy runmqckm a runmqakm na systému AIX, Linux, and Windows” na stránce 558
Tento oddíl popisuje příkazy **runmqckm** a **runmqakm** podle objektu příkazu.

ALW *Nastavení úložiště klíčů v systému AIX, Linux, and Windows*

Úložiště klíčů můžete nastavit pomocí **strmqikm** (iKeyman) Grafické rozhraní nebo z příkazového řádku pomocí příkazů **runmqckm** (iKeycmd) nebo **runmqakm** (GSKCapiCmd).

Než začnete

Úložiště klíčů je zabezpečeno heslem, protože obsahuje citlivé informace. Před vytvořením úložiště klíčů zkontrolujte volby, které produkt IBM MQ poskytuje pro bezpečné uložení hesla úložiště klíčů. Další informace viz téma “Šifrování hesel úložiště klíčů v systému AIX, Linux, and Windows” na stránce 298.

Poznámka: Deprecated V 9.3.4 Podpora úložiště klíčů CMS pro aplikace IBM MQ Java , AMQP a MQTT je zamítnuta z IBM MQ 9.3.4. Pokud používáte úložiště klíčů CMS s aplikacemi IBM MQ Java , AMQP a MQTT, měli byste migrovat na podporu úložiště klíčů PKCS#12 uvolněnou v produktu IBM MQ 9.3.0.

Nástroje **runmqckm**, **strmqikm**, **mqiptKeycmd** a **mqiptKeyman** jsou také zamítnuty. Příkaz **runmqakm** z prostředí IBM MQ a příkaz **keytool** z prostředí JRE jsou k dispozici jako alternativy.

Informace o této úloze

Připojení TLS vyžaduje na každém konci připojení *úložiště klíčů* . Každý IBM MQ správce front a IBM MQ MQI client musí mít přístup k úložišti klíčů. Další informace viz “Úložiště klíčů SSL/TLS” na stránce 25.

V systémech AIX, Linux, and Windows jsou digitální certifikáty uloženy v souboru databáze klíčů, který je spravován pomocí uživatelského rozhraní produktu **strmqikm** , nebo pomocí příkazů **runmqckm** nebo **runmqakm** . Tyto digitální certifikáty mají popisky. Specifický popisek přidruží osobní certifikát ke správci front nebo k produktu IBM MQ MQI client. TLS používá tento certifikát pro účely ověření. V systémech AIX, Linux, and Windows používá produkt IBM MQ buď hodnotu atributu **CERTLABL** , je-li nastaven, nebo výchozí hodnotu `ibmwebspheremq` s připojeným jménem správce front nebo ID přihlášení uživatele IBM MQ MQI client , a to vše malými písmeny. Podrobnosti viz Popisky digitálních certifikátů .

Název souboru databáze klíčů se skládá z cesty a názvu kmene:

- V systémech AIX and Linux je výchozí cesta pro správce front (nastavená při vytvoření správce front) `/var/mqm/qmgrs/`*`queue_manager_name`*`/ssl`.

  Na systémech Windows je výchozí cesta *`MQ_INSTALLATION_PATH`*`\Qmgrs\`*`queue_manager_name`*`\ssl`, kde *`MQ_INSTALLATION_PATH`* je adresář, ve kterém je nainstalován produkt IBM MQ . Například `C:\Program Files\IBM\MQ\Qmgrs\QM1\ssl`.

  V 9.3.0 Výchozí název souboru je `key.kdb`. Volitelně můžete použít vlastní cestu a název souboru.

  Pokud zvolíte vlastní cestu nebo název souboru, nastavte oprávnění k souboru, abyste k němu pevně řídili přístup.

- V 9.3.0 Pro klienta IBM MQ neexistuje výchozí cesta nebo název souboru. Pevně řídit přístup k tomuto souboru.

Nevytvářejte úložiště klíčů na systému souborů, který nepodporuje zámky na úrovni souborů, například NFS verze 2 na systémech Linux .

Informace o kontrole a určení názvu souboru databáze klíčů naleznete v části “Změna umístění úložiště klíčů pro správce front v systému AIX, Linux, and Windows” na stránce 301 . Název souboru databáze klíčů můžete zadat buď před, nebo po vytvoření souboru databáze klíčů.

ID uživatele, ze kterého spouštíte příkazy **strmqikm** nebo **runmqckm** , musí mít oprávnění k zápisu do adresáře, ve kterém je vytvořen nebo aktualizován soubor databáze klíčů. Pro správce front, který

používá výchozí adresář `ssl` , musí být ID uživatele, ze kterého spouštíte produkt **strmqikm** nebo **runmqckm** , členem skupiny mqm. Pokud pro systém IBM MQ MQI clientspustíte produkt **strmqikm** nebo **runmqckm** z jiného ID uživatele, než pod kterým je spuštěn klient, musíte změnit oprávnění k souboru tak, aby produkt IBM MQ MQI client mohl přistupovat k souboru databáze klíčů za běhu. Další informace viz "Přístup k souborům databáze klíčů a jejich zabezpečení v systému Windows" na stránce 299 nebo "Přístup k souborům databáze klíčů a jejich zabezpečení v systémech AIX and Linux" na stránce 299.

V produktu **strmqikm** nebo **runmqckm** pro IBM Global Security Kit (GSKit) verzi 7.0jsou nové databáze klíčů automaticky naplněny sadou předdefinovaných certifikátů certifikační autority (CA). V systému **strmqikm** nebo **runmqckm** for GSKit 8.0nejsou databáze klíčů automaticky naplněny daty, což činí počáteční nastavení bezpečnější, protože do souboru databáze klíčů zahrnete pouze požadované certifikáty CA.

Poznámka: Vzhledem k tomu, že tato změna chování pro produkt GSKit 8.0 vede k tomu, že certifikáty CA již nejsou automaticky přidávány do úložiště, musíte ručně přidat upřednostňované certifikáty CA. Tato změna chování vám poskytuje podrobnější kontrolu nad použitými certifikáty CA. Viz téma "Přidání výchozích certifikátů CA do prázdného úložiště klíčů v systému AIX, Linux, and Windows s GSKit 8.0" na stránce 300.

Databázi klíčů vytvoříte buď pomocí příkazového řádku, nebo pomocí uživatelského rozhraní **strmqikm** (iKeyman).

Poznámka: Pokud musíte spravovat certifikáty TLS způsobem, který vyhovuje standardu FIPS, použijte příkaz **runmqakm** . Uživatelské rozhraní **strmqikm** neposkytuje volbu vyhovující standardu FIPS.

Postup

Vytvořte databázi klíčů pomocí příkazového řádku.

1. Spusťte jeden z následujících příkazů:
   - Použití **runmqckm**:

     V 9.3.0 V 9.3.0
     ```
     runmqckm -keydb -create -db filename -pw password -type cms | p12 -stash
     ```
   - Použití **runmqakm**:

     V 9.3.0 V 9.3.0
     ```
     runmqakm -keydb -create -db filename -pw password -type cms | p12
     -stash -fips -strong
     ```

   kde:

   -db *název souboru*
   Určuje úplný název souboru databáze klíčů CMS.

   -pw *heslo*
   Určuje heslo pro databázi klíčů CMS V 9.3.0 V 9.3.0 nebo PKCS#12 .

   V 9.3.0 V 9.3.0 **-type *cms | p12***
   Určuje typ databáze. (Pro IBM MQmusí být `cms` nebo `pkcs12`).

   -stash
   V 9.3.0 V 9.3.0 Volitelné. Uloží heslo databáze klíčů do souboru. Tuto volbu zadejte, chcete-li uložit heslo databáze klíčů do souboru pro dočasné ukládání. Nemusíte ukládat heslo do souboru pro dočasné ukládání, pokud heslo šifrujete pomocí IBM MQ systému ochrany hesla.

   -fips (fips)
   určuje, že příkaz má být spuštěn v režimu FIPS. V režimu FIPS komponenta IBM Crypto for C (ICC) používá algoritmy, které jsou ověřeny podle standardu FIPS 140-2. Pokud se komponenta ICC neinicializuje v režimu FIPS, příkaz **runmqakm** se nezdaří.

-silné
Zkontroluje, zda zadané heslo splňuje minimální požadavky na odolnost hesla. Minimální požadavky na heslo jsou následující:

- Heslo musí mít minimální délku 14 znaků.
- Heslo musí obsahovat minimálně jedno malé písmeno, jedno velké písmeno a jednu číslici nebo speciální znak. Speciální znaky zahrnují hvězdičku (*), znak dolaru ($), znak čísla (#) a znak procenta (%). Mezera je klasifikována jako speciální znak.
- Každý znak se může v hesle vyskytovat maximálně třikrát.
- V hesle mohou být identické maximálně dva po sobě jdoucí znaky.
- Všechny znaky jsou ve standardní znakové sadě ASCII pro tisk, v rozsahu 0x20 - 0x7E.

Případně vytvořte databázi klíčů pomocí uživatelského rozhraní **strmqikm** (iKeyman).

2. V systémech AIX and Linux se přihlaste jako uživatel root. V systémech Windows se přihlaste jako administrátor nebo jako člen skupiny MQM.
3. Spusťte uživatelské rozhraní spuštěním příkazu **strmqikm** .
4. V nabídce **Soubor databáze klíčů** klepněte na volbu **Nový**.
   Otevře se okno Nový.
5. Klepněte na volbu **Typ databáze klíčů** a vyberte volbu **CMS** (Systém správy certifikátů) V 9.3.0 V 9.3.0 nebo **PKCS#12**.
6. Do pole **Název souboru** zadejte název souboru.
   Toto pole již obsahuje text key . kdb V 9.3.0 V 9.3.0 nebo key . p12. Je-li název vašeho kmene key, ponechte toto pole beze změny. Pokud jste zadali jiný název stonku, nahraďte key svým názvem stonku. .
7. Do pole **Umístění** zadejte cestu.
   Příklad:
   - Pro správce front: `/var/mqm/qmgrs/QM1/ssl` (v systémech AIX and Linux) nebo `C:\ProgramData\IBM\MQ\qmgrs\QM1\ssl` (v systémech Windows).
     Cesta musí odpovídat hodnotě atributu **SSLKeyRepository** správce front.
   - Pro IBM MQ klienta: `/var/mqm/ssl` (na systémech AIX and Linux) nebo `C:\mqm\ssl` (na systémech Windows).
8. Klepněte na tlačítko **OK**.
   Zobrazí se okno Výzva k zadání hesla.
9. Zadejte heslo do pole **Heslo** a zadejte je znovu do pole **Potvrdit heslo** .
10. V 9.3.0
    Volitelné: Chcete-li uložit heslo databáze klíčů do souboru, zaškrtněte políčko **Ukrýt heslo do souboru** .
    Tuto volbu uveďte, chcete-li uložit heslo databáze klíčů do souboru pro dočasné ukládání. Heslo nemusíte ukládat do souboru pro dočasné ukládání, pokud heslo šifrujete pomocí systému ochrany hesla IBM MQ .
11. Klepněte na tlačítko **OK**.
    Zobrazí se okno Osobní certifikáty.
12. Nastavte přístupová oprávnění podle popisu v části “Přístup k souborům databáze klíčů a jejich zabezpečení v systému Windows” na stránce 299 nebo “Přístup k souborům databáze klíčů a jejich zabezpečení v systémech AIX and Linux” na stránce 299.
13. V 9.3.0
    Pokud nepoužíváte soubor pro dočasné ukládání, zadejte heslo úložiště klíčů pro správce front nebo klientskou aplikaci podle pokynů v části “Zadání hesla úložiště klíčů pro správce front v systému AIX, Linux, and Windows” na stránce 302 nebo “Zadání hesla úložiště klíčů pro IBM MQ MQI client on AIX, Linux, and Windows” na stránce 304.

V 9.3.0 ALW V 9.3.0 *Šifrování hesel úložiště klíčů v systému AIX, Linux, and Windows*

Několik komponent produktu IBM MQ potřebuje přístup k úložišti klíčů, které obsahuje digitální certifikáty nebo symetrické klíče. Úložiště klíčů je zabezpečeno heslem, protože obsahuje citlivé informace. Heslo úložiště klíčů musí být uloženo v umístění, kde jej může produkt IBM MQ číst při přístupu k úložišti klíčů. Heslo musí být také zašifrováno, aby se snížila pravděpodobnost neoprávněného přístupu k úložišti klíčů.

Následující komponenty a funkce produktu IBM MQ podporují dvě různé metody ukládání hesel úložiště klíčů:

- Úložiště klíčů TLS správce front.
- IBM MQ MQI clients , které používají TLS.
- V 9.3.2 Nativní konfigurace vysoké dostupnosti v sekci **NativeHALocalInstance** souboru `qm.ini` .
- V 9.3.4 Konfigurace ověření tokenu v sekci **AuthToken** souboru `qm.ini` .

Hesla úložiště klíčů pro použití těmito komponentami lze šifrovat a uložit pomocí jedné z následujících metod:

Systém ochrany hesla IBM MQ .

Každá komponenta IBM MQ poskytuje příkaz k zašifrování hesla úložiště klíčů. Šifrovaný příkaz, jehož výstup příkazu je uložen v souboru.

Pro úložiště klíčů TLS správce front je heslo šifrováno, když je nastaven atribut správce front **SSLKEYRPWD** .

Heslo je šifrováno pomocí algoritmu AES-128 . Podrobnosti tohoto algoritmu jsou veřejně známé a jsou považovány za bezpečné.

Heslo je uloženo v proprietárním formátu, kterému nerozumí jiný software, který by mohl přistupovat k úložišti klíčů.

Heslo, které je šifrováno jednou komponentou IBM MQ , nemůže být použito jinou komponentou IBM MQ .

Při šifrování hesla úložiště klíčů lze poskytnout jedinečný šifrovací klíč. Jedinečný šifrovací klíč zabraňuje každému, kdo nemá přístup k šifrovacímu klíči, aby mohl dešifrovat heslo.

Heslo úložiště klíčů s prostým textem je potřebné pro správu certifikátů, které jsou v úložišti klíčů. Kromě šifrování hesla úložiště klíčů pomocí systému ochrany hesla IBM MQ musíte také uložit heslo úložiště klíčů do zabezpečeného umístění, kde k němu lze za tímto účelem přistupovat.

Další informace o systému IBM MQ pro ochranu heslem naleznete v části “Ochrana hesel v konfiguračních souborech komponenty IBM MQ” na stránce 580.

Soubor pro dočasné ukládání úložiště klíčů.

Příkazy **runmqakm** a **runmqckm** mohou uložit heslo úložiště klíčů do souboru pro dočasné ukládání.

Heslo je šifrováno proprietární metodou, která je specifická pro IBM MQ poskytovatele šifrování IBM Global Security Kit (GSKit).

Nelze poskytnout jedinečný šifrovací klíč.

Šifrované heslo je uloženo v souboru pro dočasné ukládání ve stejném adresáři jako soubor úložiště klíčů.

Kdokoli s přístupem pro čtení k úložišti klíčů i k souboru pro dočasné ukládání může přistupovat k obsahu úložiště klíčů a spravovat jej.

Bez ohledu na metodu, kterou zvolíte pro šifrování hesla úložiště klíčů, se ujistěte, že jste si vědomi omezení šifrování uložených hesel. Další informace viz téma “Omezení ochrany pomocí šifrování hesla” na stránce 588.

Související pojmy

“Zadání hesla úložiště klíčů pro správce front v systému AIX, Linux, and Windows” na stránce 302
Vzhledem k tomu, že úložiště klíčů obsahuje citlivé informace, je zabezpečeno heslem. Chcete-li mít přístup k obsahu úložiště klíčů za účelem provádění operací TLS, musí být produkt IBM MQ schopen načíst heslo úložiště klíčů.

“Zadání hesla úložiště klíčů pro IBM MQ MQI client on AIX, Linux, and Windows” na stránce 304
Vzhledem k tomu, že úložiště klíčů obsahuje citlivé informace, je zabezpečeno heslem. Chcete-li mít přístup k obsahu úložiště klíčů za účelem provádění operací TLS, musí být produkt IBM MQ schopen načíst heslo úložiště klíčů.

“Práce se zabezpečením SSL/TLS v systému AIX, Linux, and Windows” na stránce 293
V systémech AIX, Linux, and Windows je podpora TLS (Transport Layer Security) instalována spolu s produktem IBM MQ.

Windows *Přístup k souborům databáze klíčů a jejich zabezpečení v systému Windows*

Soubory databáze klíčů nemusí mít odpovídající přístupová oprávnění. Musíte nastavit odpovídající přístup k těmto souborům.

Nastavte řízení přístupu k souborům V 9.3.0 V 9.3.0 *key*.p12, *key*.kdb, *key*.sth, *key*.crla *key*.rdb, kde *klíč* je kmenový název vaší databáze klíčů, abyste udělili oprávnění omezené sadě uživatelů.

V 9.3.0 V 9.3.0 Pokud jste použili jinou příponu úložiště klíčů než .p12 nebo .kdb, musíte se také ujistit, že jsou nastavena oprávnění tohoto souboru.

Zvažte udělení přístupu takto:

úplné oprávnění
BUILTIN\Administrators, NT AUTHORITY\SYSTEM a uživatel, který vytvořil databázové soubory.

oprávnění ke čtení
Pro správce front se jedná pouze o lokální skupinu mqm. To předpokládá, že agent MCA je spuštěn pod ID uživatele ve skupině mqm.

Pro klienta se jedná o ID uživatele, pod kterým je proces klienta spuštěn.

Linux AIX *Přístup k souborům databáze klíčů a jejich zabezpečení v systémech AIX and Linux*

Soubory databáze klíčů nemusí mít odpovídající přístupová oprávnění. Musíte nastavit odpovídající přístup k těmto souborům.

Pro správce front nastavte oprávnění pro soubory databáze klíčů tak, aby je správce front a procesy kanálu mohly v případě potřeby číst, ale ostatní uživatelé je nemohou číst ani upravovat. Uživatel mqm obvykle potřebuje oprávnění ke čtení. Pokud jste vytvořili soubor databáze klíčů přihlášením jako uživatel mqm, pak jsou oprávnění pravděpodobně dostatečná; pokud jste nebyli uživatelem mqm, ale jiným uživatelem ve skupině mqm, budete pravděpodobně muset udělit oprávnění ke čtení ostatním uživatelům ve skupině mqm.

Podobně pro klienta nastavte oprávnění pro soubory databáze klíčů tak, aby je procesy aplikace klienta mohly v případě potřeby číst, ale ostatní uživatelé je nemohou číst ani upravovat. Uživatel, pod kterým je proces klienta spuštěn, obvykle potřebuje oprávnění ke čtení. Pokud jste vytvořili soubor databáze klíčů tak, že se přihlásíte jako tento uživatel, pak jsou oprávnění pravděpodobně dostatečná; pokud jste nebyli uživatelem procesu klienta, ale jiným uživatelem v této skupině, budete pravděpodobně muset udělit oprávnění ke čtení ostatním uživatelům ve skupině.

Nastavte oprávnění k souborům V 9.3.0 V 9.3.0 *key*.p12, *key*.kdb, *key*.sth, *key*.crla *key*.rdb, kde *klíč* je kmenový název databáze klíčů, na read a write pro vlastníka souboru a na read pro skupinu uživatelů mqm nebo klienta (-rw-r -----).

V 9.3.0 V 9.3.0 Pokud jste použili jinou příponu úložiště klíčů než .p12 nebo .kdb, musíte se také ujistit, že jsou nastavena oprávnění tohoto souboru.

ALW *Přidání výchozích certifikátů CA do prázdného úložiště klíčů v systému AIX, Linux, and Windows s GSKit 8.0*

Chcete-li přidat jeden nebo více výchozích certifikátů CA do prázdného úložiště klíčů s produktem IBM Global Security Kit (GSKit) verze 8.0, postupujte takto.

V produktu GSKit 7.0bylo chováním při vytváření nového úložiště klíčů automatické přidání sady výchozích certifikátů CA pro běžně používané certifikační autority. V případě systému GSKit 8.0se toto chování změnilo, takže certifikáty CA již nejsou automaticky přidávány do úložiště. Uživatel je nyní povinen ručně přidat certifikáty CA do úložiště klíčů.

Použití produktu `strmqikm`

Níže uvedené kroky proveďte na počítači, na který chcete přidat certifikát CA:

1. Spusťte grafické rozhraní pomocí příkazu **`strmqikm`** (na systému AIX, Linux, and Windows).
2. V nabídce **Soubor databáze klíčů** klepněte na volbu **Otevřít**. Otevře se okno Otevřít.
3. Klepněte na volbu **Typ databáze klíčů** a vyberte volbu **CMS** (Systém správy certifikátů) V 8.3.0 V 8.3.0 nebo PKCS#12.
4. Klepněte na tlačítko **Procházet** a přejděte do adresáře, který obsahuje soubory databáze klíčů.
5. Vyberte soubor databáze klíčů, do nějž chcete přidat certifikát, tj. například `key.kdb`.
6. Klepněte na tlačítko **Otevřít**. Otevře se okno Výzva k zadání hesla.
7. Zadejte heslo, jež jste nastavili při vytvoření databáze klíčů, a klepněte na tlačítko **OK**. Název vašeho souboru databáze klíčů se zobrazuje v poli **Název souboru**.
8. V poli **Obsah databáze klíčů** vyberte položku **Certifikáty podepsaného**.
9. Klepněte na volbu **Naplnit**. Otevře se okno Přidat certifikát CA.
10. Certifikáty CA, které jsou k dispozici pro přidání do úložiště, jsou zobrazeny v hierarchické stromové struktuře. Chcete-li zobrazit úplný seznam platných certifikátů CA, vyberte položku nejvyšší úrovně pro organizaci, jejíž certifikáty CA chcete důvěřovat.
11. Ze seznamu vyberte certifikáty CA, kterým chcete důvěřovat, a klepněte na tlačítko **OK**. Certifikáty jsou přidány do úložiště klíčů.

z příkazového řádku,

Chcete-li vypsat seznam certifikátů CA, použijte následující příkazy a pak přidejte certifikáty CA pomocí **`runmqckm`**:

- Zadáním následujícího příkazu vypište výchozí certifikáty CA spolu s organizacemi, které je vydávají:

```
runmqckm -cert -listsigners
```

- Zadejte následující příkaz pro přidání všech certifikátů CA pro organizaci uvedenou v poli *label* :

```
runmqckm -cert -populate -db filename -pw password -label label
```

kde:

`-db` *`filename`*	je úplný název cesty databáze klíčů.
`-pw` *`password`*	je heslo pro databázi klíčů.
`-label` *`label`*	je jmenovka přiložená k certifikátu.

Poznámka: Přidání certifikátu CA do úložiště klíčů vede k tomu, že produkt IBM MQ důvěřuje všem osobním certifikátům podepsaným tímto certifikátem CA. Pečlivě zvažte, kterým certifikačním autoritám chcete důvěřovat, a přidejte pouze sadu certifikátů CA potřebných k ověření klientů a správců.

Nedoporučuje se přidávat úplnou sadu výchozích certifikátů CA, pokud to není definitivní požadavek na vaši zásadu zabezpečení.

ALW *Vyhledání úložiště klíčů pro správce front v systému AIX, Linux, and Windows*

Pomocí této procedury získáte umístění souboru databáze klíčů vašeho správce front.

Postup

1. Zobrazte atributy správce front pomocí jednoho z následujících příkazů MQSC:

```
DISPLAY QMGR ALL
DISPLAY QMGR SSLKEYR
```

   Atributy správce front můžete zobrazit také pomocí příkazů IBM MQ Explorer nebo PCF.
2. Zkontrolujte výstup příkazu pro cestu a název kmene souboru databáze klíčů.
   Například:
   a. na AIX and Linux: `/var/mqm/qmgrs/QM1/ssl/key`, kde `/var/mqm/qmgrs/QM1/ssl` je cesta a `key` je název kmene
   b. na Windows: *MQ_INSTALLATION_PATH*`\qmgrs\QM1\ssl\key`, kde *MQ_INSTALLATION_PATH*`\qmgrs\QM1\ssl` je cesta a `key` je název kmene. *MQ_INSTALLATION_PATH* představuje adresář vysoké úrovně, ve kterém je nainstalován produkt IBM MQ .

Poznámka: V 9.3.0 V 9.3.0 Z IBM MQ 9.3.0 pole SSLKEYR podporuje jak úplný název souboru (včetně přípony), tak i kmenový název (bez přípony). Je-li nastaven název kmene, IBM MQ automaticky připojí `.kdb` a použije toto úložiště klíčů.

ALW *Změna umístění úložiště klíčů pro správce front v systému AIX, Linux, and Windows*

Umístění souboru databáze klíčů správce front můžete změnit různými způsoby včetně příkazu MQSC ALTER QMGR.

Umístění souboru databáze klíčů správce front můžete změnit pomocí příkazu MQSC ALTER QMGR, který nastaví atribut úložiště klíčů správce front. Například v systému AIX and Linux:

V 9.3.0 V 9.3.0

```
ALTER QMGR SSLKEYR('/var/mqm/qmgrs/QM1/ssl/MyKey.kdb')
```

V systému Windows:

V 9.3.0 V 9.3.0

```
ALTER QMGR SSLKEYR('C:\Program Files\IBM\MQ\Qmgrs\QM1\ssl\Mykey.kdb')
```

Soubor databáze klíčů má úplný název souboru: `C:\Program Files\IBM\MQ\Qmgrs\QM1\ssl\Mykey.kdb`

V 9.3.0 V 9.3.0

Upozornění: Pokud jsou v systémech Windows a Linuxpoužity kanály TLS AMQP, přípona souboru úložiště klíčů musí být jedna z následujících:

- `.kdb`, pro úložiště klíčů CMS
- `.p12` nebo `.pkcs12`pro úložiště klíčů PKCS #12 .

Atributy správce front můžete také změnit pomocí příkazů IBM MQ Explorer nebo PCF.

Změníte-li umístění souboru databáze klíčů správce front, certifikáty nebudou přeneseny ze starého umístění. Pokud je soubor databáze klíčů, ke kterému nyní přistupujete, novým souborem databáze klíčů, musíte jej naplnit potřebnými certifikáty CA a osobními certifikáty, jak je popsáno v tématu "Import osobního certifikátu do úložiště klíčů v systému AIX, Linux, and Windows" na stránce 320.

V 9.3.0 V 9.3.0 *Zadání hesla úložiště klíčů pro správce front v systému AIX, Linux, and Windows*

Vzhledem k tomu, že úložiště klíčů obsahuje citlivé informace, je zabezpečeno heslem. Chcete-li mít přístup k obsahu úložiště klíčů za účelem provádění operací TLS, musí být produkt IBM MQ schopen načíst heslo úložiště klíčů.

Produkt IBM MQ poskytuje dva mechanizmy pro zadání hesla úložiště klíčů správci front:

- "Atribut KEYRPWD" na stránce 302
- "Soubor pro dočasné ukládání úložiště klíčů" na stránce 302

Pokud nepoužíváte soubor pro dočasné ukládání úložiště klíčů, heslo úložiště klíčů je šifrováno pomocí systému ochrany hesla IBM MQ . Další informace o metodách ochrany hesla úložiště klíčů viz "Šifrování hesel úložiště klíčů v systému AIX, Linux, and Windows" na stránce 298.

Atribut KEYRPWD

Chcete-li zadat heslo úložiště klíčů přímo správci front, spusťte následující příkaz MQSC a nahraďte *heslo* heslem úložiště klíčů:

```
ALTER QMGR KEYRPWD('password')
```

Upozornění: Ujistěte se, že heslo uzavřete do apostrofů, jinak produkt IBM MQ převede znaky na velká písmena.

Je-li heslo úložiště klíčů zadáno pomocí této metody, je před uložením zašifrováno pomocí systému ochrany hesla IBM MQ .

K zašifrování hesla se používá šifrovací klíč, který je znám jako počáteční klíč. Nastavte správce front tak, aby používal jedinečný počáteční klíč k bezpečné ochraně hesla. Pokud nezadáte počáteční klíč, použije se výchozí klíč.

Před nastavením hesla úložiště klíčů zkontrolujte, zda je správce front konfigurován s použitím jedinečného počátečního klíče. Počáteční klíč můžete upravit pomocí atributu **INITKEY** v příkazu **ALTER QMGR** . Příklad:

```
ALTER QMGR INITKEY('mykey')
```

Upozornění: Úprava počátečního klíče po nastavení hesla úložiště klíčů nezpůsobí zašifrování hesla úložiště klíčů pomocí nového počátečního klíče. Změna počátečního klíče bez resetování hesla úložiště klíčů vede k tomu, že produkt IBM MQ nemůže dešifrovat heslo úložiště klíčů, a proto nemůže přistupovat k úložišti klíčů.

Další informace o atributu **KEYRPWD** viz KEYRPWD.

Soubor pro dočasné ukládání úložiště klíčů

Pokud není správci front dodáno heslo úložiště klíčů pomocí atributu **KEYRPWD** , produkt IBM MQ předpokládá, že soubor pro dočasné ukládání existuje ve stejném adresáři jako úložiště klíčů. Soubor pro dočasné ukládání má stejný kmenový název jako úložiště klíčů, ale má příponu `.sth` .

Soubor pro dočasné ukládání úložiště klíčů je vytvořen současně s úložištěm klíčů nebo později jako samostatný příkaz **runmqakm** .

Upozornění: Formát souboru pro dočasné ukládání je specifický pro IBM MQ poskytovatele šifrování IBM Global Security Kit (GSKit)a není k dispozici na platformách, které používají jiného poskytovatele šifrování.

Chcete-li vytvořit soubor pro dočasné ukládání při vytvoření úložiště klíčů, zadejte parametr **-stash** . Příklad:

```
runmqakm -keydb -create -db key.kdb -pw passw0rd -stash
```

kde *passw0rd* je heslo úložiště klíčů.

Chcete-li soubor pro dočasné ukládání vytvořit později, spusťte následující příkaz:

```
runmqakm -keydb -stashpw -db key.kdb -pw passw0rd
```

kde *passw0rd* je heslo úložiště klíčů.

Související pojmy

“Šifrování hesel úložiště klíčů v systému AIX, Linux, and Windows” na stránce 298
Několik komponent produktu IBM MQ potřebuje přístup k úložišti klíčů, které obsahuje digitální certifikáty nebo symetrické klíče. Úložiště klíčů je zabezpečeno heslem, protože obsahuje citlivé informace. Heslo úložiště klíčů musí být uloženo v umístění, kde jej může produkt IBM MQ číst při přístupu k úložišti klíčů. Heslo musí být také zašifrováno, aby se snížila pravděpodobnost neoprávněného přístupu k úložišti klíčů.

“Zadání hesla úložiště klíčů pro IBM MQ MQI client on AIX, Linux, and Windows” na stránce 304
Vzhledem k tomu, že úložiště klíčů obsahuje citlivé informace, je zabezpečeno heslem. Chcete-li mít přístup k obsahu úložiště klíčů za účelem provádění operací TLS, musí být produkt IBM MQ schopen načíst heslo úložiště klíčů.

ALW *Vyhledání úložiště klíčů pro IBM MQ MQI client na AIX, Linux, and Windows*

Umístění úložiště klíčů je dáno proměnnou MQSSLKEYR nebo je určeno ve volání MQCONNX.

Zkontrolujte proměnnou prostředí MQSSLKEYR a vyhledejte umístění souboru databáze klíčů pro IBM MQ MQI client. Příklad:

```
echo $MQSSLKEYR
```

Zkontrolujte také aplikaci, protože název souboru databáze klíčů lze nastavit také ve volání MQCONNX, jak je popsáno v tématu“Určení umístění úložiště klíčů pro IBM MQ MQI client on AIX, Linux, and Windows” na stránce 303. Hodnota nastavená ve volání MQCONNX přepíše hodnotu MQSSLKEYR.

ALW *Určení umístění úložiště klíčů pro IBM MQ MQI client on AIX, Linux, and Windows*

Pro IBM MQ MQI clientneexistuje žádné výchozí úložiště klíčů. Jeho umístění můžete určit jedním ze dvou způsobů. Ujistěte se, že k souboru databáze klíčů mohou přistupovat pouze zamýšlení uživatelé nebo administrátoři, aby se zabránilo neoprávněnému kopírování do jiných systémů.

Umístění souboru databáze klíčů pro IBM MQ MQI client můžete zadat dvěma způsoby:

- Nastavení proměnné prostředí MQSSLKEYR. Například v systému AIX and Linux:

  V 9.3.0 V 9.3.0
  ```
  export MQSSLKEYR=/var/mqm/ssl/key.kdb
  ```

  V systému Windows:

  V 9.3.0 V 9.3.0
  ```
  set MQSSLKEYR=C:\Program Files\IBM\MQ\ssl\key.kdb
  ```

- Zadání cesty a kmenového názvu souboru databáze klíčů v poli *KeyRepository* struktury MQSCO při volání MQCONNX aplikací. Další informace o použití struktury MQSCO v MQCONNX naleznete v tématu Přehled pro MQSCO.

V 9.3.0 V 9.3.0 *Zadání hesla úložiště klíčů pro IBM MQ MQI client on AIX, Linux, and Windows*

Vzhledem k tomu, že úložiště klíčů obsahuje citlivé informace, je zabezpečeno heslem. Chcete-li mít přístup k obsahu úložiště klíčů za účelem provádění operací TLS, musí být produkt IBM MQ schopen načíst heslo úložiště klíčů.

Produkt IBM MQ poskytuje čtyři mechanizmy pro dodání hesla úložiště klíčů IBM MQ MQI client:

- “Pole KeyRepoPassword modulu MQSCO ” na stránce 304
- “Proměnná prostředí MQKEYRPWD” na stránce 304
- “Atribut SSLKeyRepositoryPassword konfiguračního souboru klienta” na stránce 305
- “Soubor pro dočasné ukládání úložiště klíčů” na stránce 305

Pokud nepoužíváte soubor pro dočasné ukládání úložiště klíčů, můžete zadat heslo úložiště klíčů jako řetězec ve formátu prostého textu nebo jako řetězec, který je šifrován pomocí systému ochrany hesla IBM MQ . Další informace o metodách ochrany hesla úložiště klíčů viz “Šifrování hesel úložiště klíčů v systému AIX, Linux, and Windows” na stránce 298.

Pole KeyRepoPassword modulu MQSCO

Chcete-li zadat heslo úložiště klíčů pomocí struktury MQSCO, musíte použít kombinaci následujících tří polí řetězce proměnné:

KeyRepoPasswordLength
Délka hesla.

KeyRepoPasswordPtr
Ukazatel na umístění v paměti, které obsahuje heslo.

KeyRepoPasswordOffset
Umístění hesla v paměti reprezentované počtem bajtů od začátku struktury MQSCO.

Poznámka: Můžete dodat pouze jeden z **KeyRepoPasswordPtr** nebo **KeyRepoPasswordOffset**.

Příklad:

```
char * pwd = "passw0rd";
MQSCO  SslConnOptions = {MQSCO_DEFAULT};

SslConnOptions.KeyRepoPasswordPtr = pwd;
SslConnOptions.KeyRepoPasswordLength = (MQLONG)strlen(SslConnOptions.KeyRepoPasswordPtr);
SslConnOptions.Version = MQSCO_VERSION_6;
```

Upozornění: Zadáte-li heslo pomocí této metody, zašifrujte heslo před jeho dodáním do aplikace IBM MQ client . Další informace viz téma “Šifrování hesla úložiště klíčů” na stránce 305.

Další informace o struktuře MQCSO naleznete v tématu Volby konfigurace MQSCO-SSL/TLS.

Proměnná prostředí *MQKEYRPWD*

Pokud není klientovi dodáno heslo úložiště klíčů pomocí struktury MQSCO, můžete zadat heslo úložiště klíčů pomocí proměnné prostředí *MQKEYRPWD* . Příklad:

```
export MQKEYRPWD=passw0rd
```

, nebo

```
set MQKEYRPWD=passw0rd
```

kde `passw0rd` je vaše heslo.

Upozornění: Zadáte-li heslo pomocí této metody, před nastavením hodnoty proměnné prostředí heslo zašifrujte. Další informace viz téma “Šifrování hesla úložiště klíčů” na stránce 305.

Atribut SSLKeyRepositoryPassword konfiguračního souboru klienta

Pokud není klientovi dodáno heslo úložiště klíčů pomocí jedné z ostatních metod, můžete zadat heslo úložiště klíčů pomocí atributu **SSLKeyRepositoryPassword** v sekci **SSL** konfiguračního souboru klienta. Příklad:

```
SSL:
    SSLKeyRepositoryPassword=passw0rd
```

Upozornění: Pokud zadáte heslo pomocí této metody, zašifrujte heslo před nastavením hodnoty atributu **SSLKeyRepositoryPassword** . Další informace viz téma “Šifrování hesla úložiště klíčů” na stránce 305.

Další informace o sekci SSL konfiguračního souboru klienta viz Sekce SSL konfiguračního souboru klienta.

Soubor pro dočasné ukládání úložiště klíčů

Není-li klientovi dodáno heslo úložiště klíčů pomocí jedné z ostatních metod, produkt IBM MQ předpokládá, že soubor pro dočasné ukládání existuje ve stejném adresáři jako úložiště klíčů. Soubor pro dočasné ukládání má stejný kmenový název jako úložiště klíčů, ale má příponu `.sth` .

Soubor pro dočasné ukládání úložiště klíčů je vytvořen současně s úložištěm klíčů nebo později pomocí samostatného příkazu **runmqakm** .

Upozornění: Formát souboru pro dočasné ukládání je specifický pro IBM MQ poskytovatele šifrování IBM Global Security Kit (GSKit)a není k dispozici na platformách, které používají jiného poskytovatele šifrování.

Chcete-li vytvořit soubor pro dočasné ukládání při vytvoření úložiště klíčů, zadejte parametr **-stash** . Příklad:

```
runmqakm -keydb -create -db key.kdb -pw passw0rd -stash
```

kde *passw0rd* je heslo úložiště klíčů.

Chcete-li soubor pro dočasné ukládání vytvořit později, spusťte následující příkaz:

```
runmqakm -keydb -stashpw -db key.kdb -pw passw0rd
```

kde *passw0rd* je heslo úložiště klíčů.

Šifrování hesla úložiště klíčů

Pokud zadáte heslo úložiště klíčů pomocí jiné metody než souboru pro dočasné ukládání, zašifrujte heslo pomocí systému ochrany hesla IBM MQ . Chcete-li heslo zašifrovat, spusťte příkaz **runmqicred** . Po zobrazení výzvy zadejte heslo úložiště klíčů. Výstupem příkazu je šifrované heslo. Zašifrované heslo lze zadat do souboru IBM MQ MQI client namísto hesla ve formátu prostého textu pomocí libovolné z popsaných metod.

K zašifrování hesla se používá šifrovací klíč, který je znám jako počáteční klíč. Při šifrování hesla použijte jedinečný počáteční klíč k bezpečné ochraně hesla. Chcete-li zadat vlastní počáteční klíč, použijte parametr **-sf** příkazu **runmqicred** . Pokud nezadáte počáteční klíč, použije se výchozí klíč.

Další informace naleznete v tématu runmqicred (ochrana hesel klienta IBM MQ).

Pokud zadáte svůj vlastní počáteční klíč, když je heslo úložiště klíčů šifrováno, a zadáte zašifrované heslo do souboru IBM MQ MQI client, musíte také zajistit, že zadáte stejný počáteční klíč do souboru IBM MQ MQI client. Další informace o tom, jak poskytnout počáteční klíč pro IBM MQ MQI client, viz “Zadání počátečního klíče pro IBM MQ MQI client on AIX, Linux, and Windows” na stránce 306.

Související pojmy

“Šifrování hesel úložiště klíčů v systému AIX, Linux, and Windows” na stránce 298

Několik komponent produktu IBM MQ potřebuje přístup k úložišti klíčů, které obsahuje digitální certifikáty nebo symetrické klíče. Úložiště klíčů je zabezpečeno heslem, protože obsahuje citlivé informace. Heslo úložiště klíčů musí být uloženo v umístění, kde jej může produkt IBM MQ číst při přístupu k úložišti klíčů. Heslo musí být také zašifrováno, aby se snížila pravděpodobnost neoprávněného přístupu k úložišti klíčů.

"Zadání hesla úložiště klíčů pro správce front v systému AIX, Linux, and Windows" na stránce 302
Vzhledem k tomu, že úložiště klíčů obsahuje citlivé informace, je zabezpečeno heslem. Chcete-li mít přístup k obsahu úložiště klíčů za účelem provádění operací TLS, musí být produkt IBM MQ schopen načíst heslo úložiště klíčů.

V 9.3.0 ALW V 9.3.0 *Zadání počátečního klíče pro IBM MQ MQI client on AIX, Linux, and Windows*

Pokud zadáte proměnné pro IBM MQ MQI client , které byly zašifrovány pomocí systému IBM MQ Password Protection System, možná budete muset zadat odpovídající počáteční klíč, který byl použit k zašifrování hodnoty.

Pokud jste při šifrování hodnoty nezadali počáteční klíč, nemusíte do parametru IBM MQ clientzadávat žádnou počáteční hodnotu klíče. Pokud jste však použili jedinečný počáteční klíč, můžete poskytnout počáteční klíč produktu IBM MQ client pomocí následujících metod:

- "Zadání počátečního klíče pomocí struktury MQCSP" na stránce 306
- "Zadání počátečního klíče pomocí proměnné prostředí MQS_MQI_KEYFILE" na stránce 306
- "Zadání počátečního klíče pomocí konfiguračního souboru klienta" na stránce 307

Zadání počátečního klíče pomocí struktury MQCSP

Chcete-li zadat počáteční klíč pomocí struktury MQCSP, musíte použít kombinaci následujících tří polí řetězce proměnné:

InitialKeyLength
Délka počátečního klíče

InitialKeyPtr
Ukazatel na umístění v paměti obsahující počáteční klíč

InitialKeyOffset
Umístění počátečního klíče v paměti reprezentované počtem bajtů od začátku struktury MQCSP.

Poznámka: Můžete dodat pouze jeden z **InitialKeyPtr** nebo **InitialKeyOffset**.

Příklad:

```
char * initialKey = "myInitialKey";
MQCSP  cspOptions = {MQCSP_DEFAULT};


cspOptions.InitialKeyPtr = initialKey;
cspOptions.InitialKeyLength = (MQLONG)strlen(cspOptions.InitialKeyPtr);
cspOptions.Version = MQCSP_VERSION_2;
```

Zadání počátečního klíče pomocí proměnné prostředí MQS_MQI_KEYFILE

Není-li klientovi pomocí struktury MQCSP dodán počáteční klíč, produkt IBM MQ zkontroluje proměnnou prostředí *MQS_MQI_KEYFILE* . Tuto proměnnou prostředí byste měli nastavit na umístění souboru obsahujícího jeden řádek textu, který se skládá z počátečního klíče, který chcete použít.

Pokud například v kořenovém adresáři existuje soubor s názvem `mykey.key` a obsahuje počáteční klíč, měli byste nastavit proměnnou prostředí takto:

```
export MQS_MQI_KEYFILE=/mykey.key
```

, nebo

```
set MQS_MQI_KEYFILE=C:\mykey.key
```

Zadání počátečního klíče pomocí konfiguračního souboru klienta

Pokud není klientovi dodán počáteční klíč pomocí předchozího mechanizmu, IBM MQ zkontroluje atribut **MQIInitialKeyFile** v sekci Zabezpečení souboru `mqclient.ini` . Tento atribut byste měli nastavit na umístění souboru obsahujícího jeden řádek textu, který se skládá z počátečního klíče, který chcete použít.

Pokud například v kořenovém adresáři existuje soubor s názvem `mykey.key` a obsahuje počáteční klíč, měl by konfigurační soubor klienta obsahovat následující:

```
Security:
    MQIInitialKeyFile=/mykey.key
```

Související pojmy

“Zadání hesla úložiště klíčů pro IBM MQ MQI client on AIX, Linux, and Windows” na stránce 304
Vzhledem k tomu, že úložiště klíčů obsahuje citlivé informace, je zabezpečeno heslem. Chcete-li mít přístup k obsahu úložiště klíčů za účelem provádění operací TLS, musí být produkt IBM MQ schopen načíst heslo úložiště klíčů.

“Práce s SSL/TLS” na stránce 276
Tato témata poskytují pokyny pro provádění jednotlivých úloh souvisejících s použitím TLS s produktem IBM MQ.

ALW *Když změny certifikátů nebo úložiště certifikátů vstoupí v platnost v systému AIX, Linux, and Windows*

Změníte-li certifikáty v úložišti certifikátů nebo umístění úložiště certifikátů, změny se projeví v závislosti na typu kanálu a způsobu spuštění kanálu.

Změny certifikátů v souboru databáze klíčů a v atributu úložiště klíčů se projeví v následujících situacích:

- Když nový proces odchozího jednoho kanálu nejprve spustí kanál TLS.
- Když nový příchozí proces TCP/IP s jedním kanálem nejprve obdrží požadavek na spuštění kanálu TLS.
- Při zadání příkazu MQSC REFRESH SECURITY TYPE (SSL) pro aktualizaci prostředí TLS.
- V případě procesů aplikace klienta při zavření posledního připojení TLS v procesu. Další připojení TLS vyzvedne změny certifikátu.
- U kanálů, které jsou spuštěny jako podprocesy procesu sdružování procesů (amqrmppa), při spuštění nebo restartování procesu sdružování procesů a při prvním spuštění kanálu TLS. Pokud již proces sdružování procesů spustil kanál TLS a chcete, aby se změna okamžitě stala účinnou, spusťte příkaz MQSC REFRESH SECURITY TYPE (SSL).
- Pro kanály, které jsou spuštěny jako podprocesy inicializátoru kanálu, platí, že když je inicializátor kanálu spuštěn nebo restartován a nejprve je spuštěn kanál TLS. Pokud již proces inicializátoru kanálu spustil kanál TLS a chcete změnu provést okamžitě, spusťte příkaz MQSC REFRESH SECURITY TYPE (SSL).
- Pro kanály, které jsou spuštěny jako podprocesy modulu listener TCP/IP, platí, že když je modul listener spuštěn nebo restartován a nejprve obdrží požadavek na spuštění kanálu TLS. Pokud již modul listener spustil kanál TLS a chcete změnu provést okamžitě, spusťte příkaz MQSC REFRESH SECURITY TYPE (SSL).

Můžete také aktualizovat prostředí IBM MQ TLS pomocí příkazů IBM MQ Explorer nebo PCF.

Důležité: . Změny konfiguračního souboru úložiště klíčů a/nebo úložiště klíčů používaného zachytávačem AMS MCA (a AMS v běžném klientovi) jsou vyzvednuty při restartu správce front nebo aplikace.

ALW *Vytvoření osobního certifikátu podepsaného (svým) držitelem v systému AIX, Linux, and Windows*

Certifikát podepsaný svým držitelem můžete vytvořit pomocí konzoly **strmqikm** (iKeyman). Grafické rozhraní nebo z příkazového řádku pomocí **runmqckm** (iKeycmd) nebo **runmqakm** (GSKCapiCmd).

Poznámka: Produkt IBM MQ nepodporuje algoritmy SHA-3 nebo SHA-5 . Můžete použít názvy algoritmů digitálního podpisu SHA384WithRSA a SHA512WithRSA , protože oba algoritmy jsou členy řady SHA-2 .

Deprecated Názvy algoritmů digitálního podpisu SHA3WithRSA a SHA5WithRSA jsou zamítnuty, protože se jedná o zkrácenou formu SHA384WithRSA a SHA512WithRSA .

Další informace o tom, proč můžete chtít používat certifikáty podepsané sebou samým, naleznete v tématu Použití certifikátů podepsaných sebou samým pro vzájemné ověřování dvou správců front.

Ne všechny digitální certifikáty lze použít se všemi CipherSpecs. Ujistěte se, že jste vytvořili certifikát, který je kompatibilní se specifikacemi CipherSpecs , které potřebujete použít. Produkt IBM MQ podporuje tři různé typy CipherSpec. Podrobnosti viz “Interoperabilita specifikací Elliptic Curve a RSA CipherSpecs” na stránce 47 v tématu “Digitální certifikáty a kompatibilita CipherSpec v produktu IBM MQ” na stránce 46 .

Chcete-li použít CipherSpecs typu 1 (ty, které mají názvy začínající ECDHE_ECDSA_), musíte k vytvoření certifikátu použít příkaz **runmqakm** a musíte uvést parametr podpisového algoritmu ECDSA křivky Elliptic Curve; například **-sig_alg** EC_ecdsa_with_SHA384.

Seznam voleb, které jsou k dispozici pro hašovací algoritmus systému **-sig_alg** , naleznete v části “Volby runmqckm a runmqakm na systému AIX, Linux, and Windows” na stránce 570 .

Pokud používáte:

- Grafické rozhraní, viz “Použití uživatelského rozhraní produktu strmqikm” na stránce 308
- Příkazový řádek, viz “z příkazového řádku,” na stránce 309

ALW *Použití uživatelského rozhraní produktu **strmqikm***

Osobní certifikát můžete vytvořit pomocí **strmqikm** (iKeyman) Grafické uživatelské rozhraní.

Informace o této úloze

Produkt **strmqikm** neposkytuje volbu vyhovující standardu FIPS. Potřebujete-li spravovat certifikáty TLS způsobem, který vyhovuje standardu FIPS, použijte příkaz **runmqakm** .

Postup

Chcete-li vytvořit osobní certifikát pro svého správce front nebo produkt IBM MQ MQI client pomocí grafického uživatelského rozhraní, postupujte takto:

1. Spusťte grafické rozhraní pomocí příkazu **strmqikm** .
2. V nabídce **Soubor databáze klíčů** klepněte na volbu **Otevřít**.
   Zobrazí se okno **Otevřít** .
3. Klepněte na volbu **Typ databáze klíčů** a vyberte položku **CMS** (Certificate Management System).
4. Klepněte na tlačítko **Procházet** a přejděte do adresáře, který obsahuje soubory databáze klíčů.
5. Vyberte soubor databáze klíčů, ze kterého chcete vygenerovat požadavek; například key . kdb.
6. Klepněte na tlačítko **OK**.
   Otevře se okno **Výzva k zadání hesla** .
7. Zadejte heslo, jež jste nastavili při vytvoření databáze klíčů, a klepněte na tlačítko **OK**.
   Název vašeho souboru databáze klíčů se zobrazí v poli **Název souboru** .
8. V nabídce **Vytvořit** klepněte na volbu **Nový certifikát podepsaný svým držitelem**. Zobrazí se okno Vytvořit nový certifikát podepsaný svým držitelem.
9. Do pole **Popisek klíče** zadejte popisek certifikátu.

Popisek je buď hodnota atributu **CERTLABL** , je-li nastaven, nebo výchozí hodnota `ibmwebspheremq` s připojeným jménem správce front nebo ID uživatele pro přihlášení IBM MQ MQI client , vše malými písmeny. Podrobnosti viz Popisky digitálních certifikátů .

10. Zadejte nebo vyberte hodnotu pro libovolné pole v poli **Rozlišující název** nebo v polích **Alternativní název předmětu** .
11. Pro zbývající pole buď přijměte výchozí hodnoty, nebo zadejte nebo vyberte nové hodnoty.

    Další informace o rozlišujících názvech naleznete v části “Rozlišující názvy” na stránce 14.
12. Klepněte na tlačítko **OK**.

    Seznam **Osobní certifikáty** zobrazuje popisek vámi vytvořeného osobního certifikátu podepsaného sebou samým.

ALW *z příkazového řádku,*

Osobní certifikát můžete vytvořit z příkazového řádku pomocí příkazů **runmqckm** (iKeycmd) nebo **runmqakm** (GSKCapiCmd). Potřebujete-li spravovat certifikáty SSL nebo TLS způsobem, který vyhovuje standardu FIPS, použijte příkaz **runmqakm** .

Postup

Vytvořte osobní certifikát podepsaný svým držitelem pomocí příkazu **runmqckm** nebo **runmqakm** (GSKCapiCmd).

- Použití **runmqckm**:

```
runmqckm -cert -create -db filename -pw password -label label
         -dn distinguished_name -size key_size
         -x509version version -expire days -sig_alg algorithm
```

Místo `-dn` *`distinguished_name`*můžete použít `-san_dnsname` *`DNS_names`*, `-san_emailaddr` *`email_addresses`*nebo `-san_ipaddr` *`IP_addresses`*.

- Použití **runmqakm**:

```
runmqakm -cert -create -db filename -pw password -label label
         -dn distinguished_name -size key_size
         -x509version version -expire days -fips -sig_alg algorithm
```

kde:

-db *název souboru*
Určuje úplný název souboru databáze klíčů CMS .

-pw *heslo*
Určuje heslo pro databázi klíčů CMS .

-label *popisek*
Určuje popisek klíče připojený k certifikátu. Popisek je buď hodnota atributu **CERTLABL** , je-li nastaven, nebo výchozí hodnota `ibmwebspheremq` s připojeným jménem správce front nebo ID uživatele pro přihlášení IBM MQ MQI client , vše malými písmeny. Podrobnosti viz “Digitální štítky certifikátů, pochopení požadavků” na stránce 26.

-dn *název_rozlišení*
Uvádí rozlišující název X.500 uzavřený v uvozovkách. Je vyžadován alespoň jeden atribut. Můžete dodat více atributů organizační jednotky a DC.

Poznámka: nástroje **runmqckm** a **runmqakm** odkazují na atribut PSČ `POSTALCODE`, nikoli `PC`. Při použití těchto příkazů správy certifikátů k vyžádání certifikátů s poštovním kódem vždy zadejte do parametru **-dn** hodnotu `POSTALCODE` .

-size *velikost_klíče*
Určuje velikost klíče. Pokud používáte **runmqckm**, hodnota může být 512 nebo 1024. Pokud používáte **runmqakm**, hodnota může být 512, 1024nebo 2048.

x509version *verze*
Verze certifikátu X.509 , který má být vytvořen. Hodnota může být 1, 2 nebo 3. Výchozí hodnota je 3.

-file *název_souboru*
Určuje název souboru pro žádost o certifikát.

-expire *dny*
Čas vypršení platnosti certifikátu ve dnech. Výchozí hodnota je 365 dní pro certifikát.

-fips (fips)
určuje, že příkaz má být spuštěn v režimu FIPS. Používá se pouze komponenta FIPS IBM Crypto for C (ICC) a tato komponenta musí být úspěšně inicializována v režimu FIPS. V režimu FIPS komponenta ICC používá algoritmy, které byly ověřeny podle standardu FIPS 140-2. Pokud se komponenta ICC neinicializuje v režimu FIPS, příkaz **runmqakm** se nezdaří.

-sig_alg
Pro parametr **runmqckm**uvádí asymetrický podpisový algoritmus použitý pro vytvoření dvojice klíčů položky. Hodnota může být MD2_WITH_RSA, MD2WithRSA, MD5_WITH_RSA, MD5WithRSA, SHA1WithDSA, SHA1WithECDSA, SHA1WithRSA, SHA2/ECDSA, SHA224WithECDSA, SHA256_WITH_RSA, SHA256WithECDSA, SHA256WithRSA, SHA2WithECDSA, SHA3/ECDSA, SHA384_WITH_RSA, SHA384WithECDSA, SHA384WithRSA, SHA3WithECDSA, SHA5/ECDSA, SHA512_WITH_RSA, SHA512WithECDSA, SHA512WithRSA, SHA5WithECDSA, SHA_WITH_DSA, SHA_WITH_RSA, SHAWithDSA, SHAWithRSA. Výchozí hodnota je SHA1WithRSA.

-sig_alg
Pro parametr **runmqakm**určuje hašovací algoritmus používaný při vytváření žádosti o certifikát. Tento hašovací algoritmus se používá k vytvoření podpisu přidruženého k nově vytvořené žádosti o certifikát. Hodnota může být md5, MD5_WITH_RSA, MD5WithRSA, SHA_WITH_DSA, SHA_WITH_RSA, sha1, SHA1WithDSA, SHA1WithECDSA, SHA1WithRSA, sha224, SHA224_WITH_RSA, SHA224WithDSA, SHA224WithECDSA, SHA224WithRSA, sha256, SHA256_WITH_RSA, SHA256WithDSA, SHA256WithECDSA, SHA256WithRSA, SHA2WithRSA, sha384, SHA384_WITH_RSA, SHA384WithECDSA, SHA384WithRSA, sha512, SHA512_WITH_RSA, SHA512WithECDSA, SHA512WithRSA, SHAWithDSA, SHAWithRSA, EC_ecdsa_with_SHA1, EC_ecdsa_with_SHA224, EC_ecdsa_with_SHA256, EC_ecdsa_with_SHA384nebo EC_ecdsa_with_SHA512. Výchozí hodnota je SHA1WithRSA.

-san_dnsname *DNS_names*
Určuje seznam názvů DNS pro vytvářenou položku oddělených čárkami nebo mezerami.

-san_emailaddr *email_addresses*
Určuje seznam e-mailových adres pro vytvářenou položku oddělených čárkami nebo mezerami.

-san_ipaddr *adresa_IP*
Určuje seznam adres IP pro vytvářený záznam oddělených čárkami nebo mezerami.

ALW *Vyžádání osobního certifikátu na AIX, Linux, and Windows*

Osobní certifikát si můžete vyžádat pomocí konzoly **strmqikm** (iKeyman). Grafické rozhraní nebo z příkazového řádku pomocí příkazů **runmqckm** (iKeycmd) nebo **runmqakm** (GSKCapiCmd). Potřebujete-li spravovat certifikáty SSL nebo TLS způsobem, který vyhovuje standardu FIPS, použijte příkaz **runmqakm** .

Informace o této úloze

Osobní certifikát si můžete vyžádat pomocí grafického rozhraní produktu **strmqikm** nebo z příkazového řádku s následujícími aspekty:

- Produkt IBM MQ nepodporuje algoritmy SHA-3 nebo SHA-5 . Můžete použít názvy algoritmů digitálního podpisu SHA384WithRSA a SHA512WithRSA , protože oba algoritmy jsou členy řady SHA-2 .
- Deprecated Názvy algoritmů digitálního podpisu SHA3WithRSA a SHA5WithRSA jsou zamítnuty, protože se jedná o zkrácenou formu SHA384WithRSA a SHA512WithRSA .
- Ne všechny digitální certifikáty lze použít se všemi CipherSpecs. Ujistěte se, že požadujete certifikát, který je kompatibilní se specifikacemi CipherSpecs , které potřebujete použít. Produkt IBM MQ podporuje tři různé typy CipherSpec. Podrobnosti viz “Interoperabilita specifikací Elliptic Curve a RSA

CipherSpecs” na stránce 47 v tématu “Digitální certifikáty a kompatibilita CipherSpec v produktu IBM MQ” na stránce 46 .

- Chcete-li použít CipherSpecs typu 1 (s názvy začínajícími ECDHE_ECDSA_), musíte k vyžádání certifikátu použít příkaz **runmqakm** a musíte uvést parametr podpisového algoritmu ECDSA Elliptic Curve; například **-sig_alg** EC_ecdsa_with_SHA384.

  Seznam voleb, které jsou k dispozici pro hašovací algoritmus systému **-sig_alg** , naleznete v části “Volby runmqckm a runmqakm na systému AIX, Linux, and Windows” na stránce 570 .
- Pouze příkaz **runmqakm** poskytuje volbu vyhovující standardu FIPS.
- Pokud používáte kryptografický hardware, viz “Vyžádání osobního certifikátu pro hardware PKCS #11” na stránce 329.

Pokud používáte:

- Grafické rozhraní, viz “Použití uživatelského rozhraní produktu strmqikm” na stránce 311
- Příkazový řádek, viz “z příkazového řádku,” na stránce 312

ALW *Použití uživatelského rozhraní produktu **strmqikm***

Osobní certifikát si můžete vyžádat pomocí konzoly **strmqikm** (iKeyman). Grafické uživatelské rozhraní. Potřebujete-li spravovat certifikáty SSL nebo TLS způsobem, který vyhovuje standardu FIPS, použijte příkaz **runmqakm** .

Informace o této úloze

Produkt **strmqikm** neposkytuje volbu vyhovující standardu FIPS. Potřebujete-li spravovat certifikáty TLS způsobem, který vyhovuje standardu FIPS, použijte příkaz **runmqakm** .

Postup

Chcete-li požádat o osobní certifikát pomocí uživatelského rozhraní iKeyman , postupujte takto:

1. Spusťte uživatelské rozhraní pomocí příkazu **strmqikm** .
2. V nabídce **Soubor databáze klíčů** klepněte na volbu **Otevřít**.

   Otevře se okno **Otevřít**.
3. Klepněte na volbu **Typ databáze klíčů** a vyberte položku **CMS** (Certificate Management System).
4. Klepněte na tlačítko **Procházet** a přejděte do adresáře, který obsahuje soubory databáze klíčů.
5. Vyberte soubor databáze klíčů, ze kterého chcete vygenerovat požadavek; například key.kdb.
6. Klepněte na tlačítko **Otevřít**.

   Otevře se okno **Výzva k zadání hesla** .
7. Zadejte heslo, jež jste nastavili při vytvoření databáze klíčů, a klepněte na tlačítko **OK**.

   Název vašeho souboru databáze klíčů se zobrazí v poli **Název souboru** .
8. V nabídce **Vytvořit** klepněte na volbu **Nová žádost o certifikát**. Otevře se okno **Vytvořit nový klíč a žádost o certifikát** .
9. Do pole **Popisek klíče** zadejte popisek certifikátu.

   Popisek je buď hodnota atributu **CERTLABL** , je-li nastaven, nebo výchozí hodnota ibmwebspheremq s připojeným jménem správce front nebo ID uživatele pro přihlášení IBM MQ MQI client , vše malými písmeny. Podrobnosti viz Popisky digitálních certifikátů .
10. Zadejte nebo vyberte hodnotu pro libovolné pole v poli **Rozlišující název** nebo v polích **Alternativní název předmětu** . Pro zbývající pole buď přijměte výchozí hodnoty, nebo zadejte nebo vyberte nové hodnoty.

    Další informace o rozlišujících názvech naleznete v části “Rozlišující názvy” na stránce 14.
11. Do pole **Zadejte název souboru, do kterého se má uložit žádost o certifikát** buď přijměte předvolbu certreq.arm, nebo zadejte novou hodnotu s úplnou cestou.
12. Klepněte na tlačítko **OK**.

    Zobrazí se potvrzovací okno.

13. Klepněte na tlačítko **OK**.

    Seznam **Požadavky na osobní certifikát** zobrazuje popisek nové žádosti o osobní certifikát, kterou jste vytvořili. Žádost o certifikát je uložena v souboru, který jste vybrali v kroku “11” na stránce 311.
14. Požádejte o nový osobní certifikát buď odesláním souboru certifikační autoritě (CA), nebo zkopírováním souboru do formuláře požadavku na webu certifikační autority.

ALW *z příkazového řádku,*

Osobní certifikát můžete vyžádat z příkazového řádku pomocí příkazů **runmqckm** (iKeycmd) nebo **runmqakm** (GSKCapiCmd). Potřebujete-li spravovat certifikáty SSL nebo TLS způsobem, který vyhovuje standardu FIPS, použijte příkaz **runmqakm** .

Postup

Vyžádejte si osobní certifikát pomocí příkazu **runmqckm** nebo **runmqakm** (GSKCapiCmd).

- Použití **runmqckm**:

```
runmqckm -certreq -create -db filename -pw
password -label label
         -dn distinguished_name -size key_size
        -file filename -sig_alg algorithm
```

  Místo -dn *distinguished_name*můžete použít -san_dsname *DNS_names*, -san_emailaddr *email_addresses*nebo -san_ipaddr *IP_addresses*.

- Použití **runmqakm**:

```
runmqakm -certreq -create -db filename -pw
password -label label
         -dn distinguished_name -size key_size
         -file filename -fips -sig_alg algorithm
```

kde:

-db *název souboru*
Určuje úplný název souboru databáze klíčů CMS .

-pw *heslo*
Určuje heslo pro databázi klíčů CMS .

-label *popisek*
Určuje popisek klíče připojený k certifikátu. Popisek je buď hodnota atributu **CERTLABL** , je-li nastaven, nebo výchozí hodnota ibmwebspheremq s připojeným jménem správce front nebo ID uživatele pro přihlášení IBM MQ MQI client , vše malými písmeny. Podrobnosti viz “Digitální štítky certifikátů, pochopení požadavků” na stránce 26.

-dn *název_rozlišení*
Uvádí rozlišující název X.500 uzavřený v uvozovkách. Je vyžadován alespoň jeden atribut. Můžete dodat více atributů organizační jednotky a DC.

Poznámka: nástroje **runmqckm** a **runmqakm** odkazují na atribut PSČ POSTALCODE, nikoli PC. Při použití těchto příkazů správy certifikátů k vyžádání certifikátů s poštovním kódem vždy zadejte do parametru **-dn** hodnotu POSTALCODE .

-size *velikost_klíče*
Určuje velikost klíče. Pokud používáte **runmqckm**, hodnota může být 512 nebo 1024. Pokud používáte **runmqakm**, hodnota může být 512, 1024nebo 2048.

-file *název_souboru*
Určuje název souboru pro žádost o certifikát.

-fips (fips)
určuje, že příkaz má být spuštěn v režimu FIPS. V režimu FIPS komponenta IBM Crypto for C (ICC) používá algoritmy, které jsou ověřeny podle standardu FIPS 140-2. Pokud se komponenta ICC neinicializuje v režimu FIPS, příkaz **runmqakm** se nezdaří.

-sig_alg
Pro parametr **runmqckm**uvádí asymetrický podpisový algoritmus použitý pro vytvoření dvojice klíčů položky. Hodnota může být MD2_WITH_RSA, MD2WithRSA, MD5_WITH_RSA, MD5WithRSA, SHA1WithDSA, SHA1WithECDSA, SHA1WithRSA, SHA2/ECDSA, SHA224WithECDSA, SHA256_WITH_RSA, SHA256WithECDSA, SHA256WithRSA, SHA2WithECDSA, SHA3/ECDSA, SHA384_WITH_RSA, SHA384WithECDSA, SHA384WithRSA, SHA3WithECDSA, SHA5/ECDSA, SHA512_WITH_RSA, SHA512WithECDSA, SHA512WithRSA, SHA5WithECDSA, SHA_WITH_DSA, SHA_WITH_RSA, SHAWithDSA, SHAWithRSA. Výchozí hodnota je SHA1WithRSA.

-sig_alg
Pro parametr **runmqakm**určuje hašovací algoritmus používaný při vytváření žádosti o certifikát. Tento hašovací algoritmus se používá k vytvoření podpisu přidruženého k nově vytvořené žádosti o certifikát. Hodnota může být md5, MD5_WITH_RSA, MD5WithRSA, SHA_WITH_DSA, SHA_WITH_RSA, sha1, SHA1WithDSA, SHA1WithECDSA, SHA1WithRSA, sha224, SHA224_WITH_RSA, SHA224WithDSA, SHA224WithECDSA, SHA224WithRSA, sha256, SHA256_WITH_RSA, SHA256WithDSA, SHA256WithECDSA, SHA256WithRSA, SHA2WithRSA, sha384, SHA384_WITH_RSA, SHA384WithECDSA, SHA384WithRSA, sha512, SHA512_WITH_RSA, SHA512WithECDSA, SHA512WithRSA, SHAWithDSA, SHAWithRSA, EC_ecdsa_with_SHA1, EC_ecdsa_with_SHA224, EC_ecdsa_with_SHA256, EC_ecdsa_with_SHA384nebo EC_ecdsa_with_SHA512. Výchozí hodnota je SHA1WithRSA.

-san_dnsname *DNS_names*
Určuje seznam názvů DNS pro vytvářenou položku oddělených čárkami nebo mezerami.

-san_emailaddr *email_addresses*
Určuje seznam e-mailových adres pro vytvářenou položku oddělených čárkami nebo mezerami.

-san_ipaddr *adresa_IP*
Určuje seznam adres IP pro vytvářený záznam oddělených čárkami nebo mezerami.

Jak pokračovat dále

Odešlete žádost o certifikát certifikační autoritě. Další informace viz “Příjem osobních certifikátů do úložiště klíčů v systému AIX, Linux, and Windows” na stránce 315.

ALW *Obnovení existujícího osobního certifikátu v systému AIX, Linux, and Windows*

Osobní certifikát můžete obnovit pomocí konzoly **strmqikm** (iKeyman). Grafické rozhraní nebo z příkazového řádku pomocí příkazů **runmqckm** (iKeycmd) nebo **runmqakm** (GSKCapiCmd).

Informace o této úloze

Pokud máte požadavek na použití větších velikostí klíčů pro vaše osobní certifikáty, nemůžete existující certifikát obnovit. Chcete-li vytvořit novou žádost o certifikát, která bude používat požadované velikosti klíčů, musíte nahradit existující klíč podle postupu popsaného v části “Vyžádání osobního certifikátu na AIX, Linux, and Windows” na stránce 310 .

Osobní certifikát má datum vypršení platnosti, po kterém již nelze certifikát používat. Tato úloha vysvětluje, jak obnovit existující osobní certifikát před jeho vypršením.

*Použití uživatelského rozhraní produktu **strmqikm***

Informace o této úloze

Produkt **strmqikm** neposkytuje volbu vyhovující standardu FIPS. Potřebujete-li spravovat certifikáty TLS způsobem, který vyhovuje standardu FIPS, použijte příkaz **runmqakm** .

Postup

Chcete-li požádat o osobní certifikát pomocí uživatelského rozhraní produktu **strmqikm** , postupujte takto:

1. Spusťte uživatelské rozhraní pomocí příkazu **strmqikm** na systému AIX, Linux, and Windows.
2. V nabídce **Soubor databáze klíčů** klepněte na volbu **Otevřít**.
   Otevře se okno **Otevřít**.
3. Klepněte na volbu **Typ databáze klíčů** a vyberte položku **CMS** (Certificate Management System).
4. Klepněte na tlačítko **Procházet** a přejděte do adresáře, který obsahuje soubory databáze klíčů.
5. Vyberte soubor databáze klíčů, ze kterého chcete vygenerovat požadavek; například `key.kdb`.
6. Klepněte na tlačítko **Otevřít**.
   Otevře se okno **Výzva k zadání hesla** .
7. Zadejte heslo, jež jste nastavili při vytvoření databáze klíčů, a klepněte na tlačítko **OK**.
   Název vašeho souboru databáze klíčů se zobrazí v poli **Název souboru** .
8. V rozevírací nabídce vyberte volbu **Osobní certifikáty** a vyberte certifikát ze seznamu, který chcete obnovit.
9. Klepněte na volbu **Znovu vytvořit požadavek ...** .
   Otevře se okno, ve kterém můžete zadat název souboru a informace o umístění souboru.
10. Do pole **název souboru** buď přijměte výchozí hodnotu `certreq.arm`, nebo zadejte novou hodnotu včetně úplné cesty k souboru.
11. Klepněte na tlačítko **OK**. Žádost o certifikát je uložena v souboru, který jste vybrali v kroku “9” na stránce 314.
12. Požádejte o nový osobní certifikát buď odesláním souboru certifikační autoritě (CA), nebo zkopírováním souboru do formuláře požadavku na webu certifikační autority.

z příkazového řádku,

Postup

K vyžádání osobního certifikátu pomocí příkazu **runmqckm** nebo **runmqakm** použijte následující příkazy:

- Použití **runmqckm**:

```
runmqckm -certreq -recreate -db filename -pw
password -label label
-target filename
```

- Použití příkazu runmqakm:

```
runmqakm -certreq -recreate -db filename -pw
password -label label
-target filename
```

kde:

-db *název souboru*
Určuje úplný název souboru databáze klíčů CMS .

-pw *heslo*
Určuje heslo pro databázi klíčů CMS .

-target *název_souboru*
Určuje název souboru pro žádost o certifikát.

Poznámka: Vzhledem k tomu, že staré informace o certifikátu jsou v mezipaměti, musíte spustit příkaz REFRESH SECURITY TYPE (SSL).

Jak pokračovat dále

Jakmile od certifikační autority obdržíte podepsaný osobní certifikát, můžete jej přidat do databáze klíčů pomocí kroků popsaných v části “Příjem osobních certifikátů do úložiště klíčů v systému AIX, Linux, and Windows” na stránce 315.

ALW *Příjem osobních certifikátů do úložiště klíčů v systému AIX, Linux, and Windows*

Pomocí této procedury obdržíte osobní certifikát do souboru databáze klíčů. Úložiště klíčů musí být stejné jako úložiště, kde jste vytvořili žádost o certifikát.

Poté, co vám certifikační autorita odešle nový osobní certifikát, přidejte jej do souboru databáze klíčů, ze kterého jste vygenerovali novou žádost o certifikát. Pokud certifikační autorita odešle certifikát jako součást e-mailové zprávy, zkopírujte certifikát do samostatného souboru.

Použití produktu `strmqikm`

Potřebujete-li spravovat certifikáty TLS způsobem, který vyhovuje standardu FIPS, použijte příkaz **runmqakm** . Produkt **strmqikm** neposkytuje volbu vyhovující standardu FIPS.

Ujistěte se, že soubor certifikátů, který má být importován, má oprávnění k zápisu pro aktuálního uživatele, a poté použijte následující proceduru pro správce front nebo IBM MQ MQI client k přijetí osobního certifikátu do souboru databáze klíčů:

1. Spusťte grafické rozhraní pomocí příkazu **strmqikm** .
2. V nabídce **Soubor databáze klíčů** klepněte na volbu **Otevřít**. Otevře se okno Otevřít.
3. Klepněte na volbu **Typ databáze klíčů** a vyberte položku **CMS** (Certificate Management System).
4. Klepněte na tlačítko **Procházet** a přejděte do adresáře, který obsahuje soubory databáze klíčů.
5. Vyberte soubor databáze klíčů, do nějž chcete přidat certifikát, tj. například `key.kdb`.
6. Klepněte na volbu **Otevřít**a poté klepněte na tlačítko **OK**. Otevře se okno Výzva k zadání hesla.
7. Zadejte heslo, jež jste nastavili při vytvoření databáze klíčů, a klepněte na tlačítko **OK**. Název vašeho souboru databáze klíčů se zobrazí v poli **Název souboru** . Vyberte pohled **Osobní certifikáty** .
8. Klepněte na tlačítko **Přijmout**. Otevře se okno Přijmout certifikát ze souboru.
9. Zadejte název souboru certifikátů a umístění nového osobního certifikátu nebo klepněte na tlačítko **Procházet** a vyberte název a umístění.
10. Klepněte na tlačítko **OK**. Pokud již máte osobní certifikát v databázi klíčů, otevře se okno s dotazem, zda chcete nastavit klíč, který přidáváte jako výchozí klíč v databázi.
11. Klepněte na volbu **Ano** nebo **Ne**. Otevře se okno Zadat jmenovku.
12. Klepněte na tlačítko **OK**. Pole **Osobní certifikáty** zobrazuje popisek nového osobního certifikátu, který jste přidali.

z příkazového řádku,

Chcete-li přidat osobní certifikát do souboru databáze klíčů, použijte jeden z následujících příkazů:

- Použití **runmqckm**:

```
runmqckm -cert -receive -file filename -db filename -pw password
         -format ascii
```

- Použití **runmqakm**:

```
runmqakm -cert -receive -file filename -db filename -pw password -fips
```

kde:

-file ***název_souboru***
Určuje úplný název souboru osobního certifikátu.

-db ***název souboru***
Určuje úplný název souboru databáze klíčů CMS .

-pw ***heslo***
Určuje heslo pro databázi klíčů CMS .

-format ***ve formátu ASCII***
Určuje formát certifikátu. Hodnota může být `ascii` pro ASCII kódované formátem Base64 nebo `binary` pro binární data DER. Výchozí hodnota: `ascii`.

-fips (fips)
určuje, že příkaz má být spuštěn v režimu FIPS. V režimu FIPS komponenta IBM Crypto for C (ICC) používá algoritmy, které byly ověřeny podle standardu FIPS 140-2. Pokud se komponenta ICC neinicializuje v režimu FIPS, příkaz **runmqakm** se nezdaří.

Pokud používáte kryptografický hardware, postupujte podle pokynů v části "Příjem osobního certifikátu do hardwaru PKCS #11" na stránce 330.

ALW *Extrakce certifikátu CA z úložiště klíčů v systému AIX, Linux, and Windows*

Chcete-li extrahovat certifikát CA, postupujte podle tohoto postupu.

Použití produktu `strmqikm`

Potřebujete-li spravovat certifikáty TLS způsobem, který vyhovuje standardu FIPS, použijte příkaz **runmqakm** . **strmqikm** (iKeyman) neposkytuje volbu vyhovující standardu FIPS.

Na počítači, ze kterého chcete extrahovat certifikát CA, postupujte takto:

1. Spusťte grafické rozhraní pomocí příkazu **strmqikm** .
2. V nabídce **Soubor databáze klíčů** klepněte na volbu **Otevřít**. Otevře se okno Otevřít.
3. Klepněte na volbu **Typ databáze klíčů** a vyberte položku **CMS** (Certificate Management System).
4. Klepněte na tlačítko **Procházet** a přejděte do adresáře, který obsahuje soubory databáze klíčů.
5. Vyberte soubor databáze klíčů, ze kterého chcete extrahovat, například `key.kdb`.
6. Klepněte na tlačítko **Otevřít**. Otevře se okno Výzva k zadání hesla.
7. Zadejte heslo, jež jste nastavili při vytvoření databáze klíčů, a klepněte na tlačítko **OK**. Název vašeho souboru databáze klíčů se zobrazí v poli **Název souboru** .
8. V poli **Obsah databáze klíčů** vyberte volbu **Certifikáty podepsaného** a vyberte certifikát, který chcete extrahovat.
9. Klepněte na volbu **Extrahovat**. Otevře se okno Extrahovat certifikát do souboru.
10. Vyberte **Datový typ** certifikátu, například **Base64-encoded** pro soubor s příponou `.arm` .
11. Zadejte název souboru certifikátů a umístění, kam chcete certifikát uložit, nebo klepněte na tlačítko **Procházet** a vyberte název a umístění.
12. Klepněte na tlačítko **OK**. Certifikát se zapíše do souboru, který jste uvedli.

z příkazového řádku,

Pomocí následujících příkazů extrahujte certifikát CA pomocí příkazu **runmqckm** nebo **runmqakm** :

```
runmqckm -cert -extract -db filename -pw password -label label
         -target filename -format ascii
```

, nebo

```
runmqakm -cert -extract -db filename -pw password -label label
         -target filename -format ascii -fips
```

kde:

`-db` *`filename`*	je úplný název cesty databáze klíčů CMS .
`-pw` *`password`*	je heslo pro databázi klíčů CMS.
`-label` *`label`*	je jmenovka přiložená k certifikátu.
`-target` *`filename`*	je název cílového souboru.
`-format` *`ascii`*	je formát certifikátu. Hodnota může být `ascii` pro ASCII kódované formátem Base64 nebo `binary` pro binární data DER. Výchozí hodnota: `ascii`.
`-fips`	určuje, že příkaz má být spuštěn v režimu FIPS. V režimu FIPS komponenta IBM Crypto for C (ICC) používá algoritmy, které byly ověřeny podle standardu FIPS 140-2. Pokud se komponenta ICC neinicializuje v režimu FIPS, příkaz **runmqakm** se nezdaří.

ALW *Extrakce veřejné části certifikátu podepsaného (svým) držitelem z úložiště klíčů v systému AIX, Linux, and Windows*

Postupujte podle tohoto postupu, chcete-li extrahovat veřejnou část certifikátu podepsaného (svým) držitelem.

Použití produktu `strmqikm`

Potřebujete-li spravovat certifikáty TLS způsobem, který vyhovuje standardu FIPS, použijte příkaz **runmqakm** . **strmqikm** (iKeyman) neposkytuje volbu vyhovující standardu FIPS.

Na počítači, ze kterého chcete extrahovat veřejnou část certifikátu podepsaného (svým) držitelem, postupujte takto:

1. Spusťte grafické rozhraní pomocí příkazu **strmqikm** .
2. V nabídce **Soubor databáze klíčů** klepněte na volbu **Otevřít**. Otevře se okno Otevřít.
3. Klepněte na volbu **Typ databáze klíčů** a vyberte položku **CMS** (Certificate Management System).
4. Klepněte na tlačítko **Procházet** a přejděte do adresáře, který obsahuje soubory databáze klíčů.
5. Vyberte soubor databáze klíčů, ze kterého chcete extrahovat certifikát, například `key.kdb`.
6. Klepněte na tlačítko **OK**. Otevře se okno Výzva k zadání hesla.
7. Zadejte heslo, jež jste nastavili při vytvoření databáze klíčů, a klepněte na tlačítko **OK**. Název vašeho souboru databáze klíčů se zobrazí v poli **Název souboru** .
8. V poli **Obsah databáze klíčů** vyberte volbu **Osobní certifikáty** a vyberte certifikát.
9. Klepněte na volbu **Extrahovat certifikát**. Otevře se okno Extrahovat certifikát do souboru.
10. Vyberte **Datový typ** certifikátu, například **Base64-encoded** pro soubor s příponou `.arm` .
11. Zadejte název souboru certifikátů a umístění, kam chcete certifikát uložit, nebo klepněte na tlačítko **Procházet** a vyberte název a umístění.
12. Klepněte na tlačítko **OK**. Certifikát se zapíše do souboru, který jste uvedli. Všimněte si, že když extrahujete (spíše než exportujete) certifikát, je zahrnuta pouze veřejná část certifikátu, takže heslo není vyžadováno.

z příkazového řádku,

Pomocí následujících příkazů extrahujte veřejnou část certifikátu podepsaného (svým) držitelem pomocí **runmqckm** nebo **runmqakm**:

- Použití příkazu runmqckm:

```
runmqckm -cert -extract -db filename -pw password -label label -target filename
         -format ascii
```

- Použití příkazu runmqakm:

```
runmqakm -cert -extract -db filename -pw password -label label
            -target filename -format ascii -fips
```

kde:

`-db filename`	je úplný název cesty databáze klíčů CMS .
`-pw password`	je heslo pro databázi klíčů CMS.
`-label label`	je jmenovka přiložená k certifikátu.
`-target filename`	je název cílového souboru.
`-format ascii`	je formát certifikátu. Hodnota může být `ascii` pro ASCII kódované formátem Base64 nebo `binary` pro binární data DER. Výchozí hodnota: `ascii`.
`-fips`	určuje, že příkaz má být spuštěn v režimu FIPS. V režimu FIPS komponenta IBM Crypto for C (ICC) používá algoritmy, které byly ověřeny podle standardu FIPS 140-2. Pokud se komponenta ICC neinicializuje v režimu FIPS, příkaz **runmqakm** se nezdaří.

ALW *Přidání certifikátu CA nebo veřejné části certifikátu podepsaného držitelem do úložiště klíčů v systému AIX, Linux, and Windows*

Tento postup popisuje přidání certifikátu CA nebo veřejné části certifikátu podepsaného (svým) držitelem do úložiště klíčů.

Je-li certifikát, který chcete přidat, v řetězu certifikátů, musíte přidat rovněž všechny certifikáty, které jsou v řetězu certifikátů nad tímto certifikátem. Certifikáty musíte přidat v přísně sestupném pořadí počínaje kořenem a pokračujíce certifikátem CA, který v řetězu bezprostředně následuje pod ním atd..

Je-li v pokynech zmíněn certifikát CA, platí tento pokyn rovněž pro veřejnou část certifikátu podepsaného (svým) držitelem.

Poznámka: Musíte se ujistit, že je certifikát v kódování ASCII (UTF-8) nebo v binárním kódování (DER), protože produkt IBM Global Security Kit (GSKit) nepodporuje certifikáty s jinými typy kódování.

Použití produktu `strmqikm`

Potřebujete-li spravovat certifikáty TLS způsobem, který vyhovuje standardu FIPS, použijte příkaz **runmqakm** . Produkt **strmqikm** neposkytuje volbu vyhovující standardu FIPS.

Níže uvedené kroky proveďte na počítači, na který chcete přidat certifikát CA:

1. Spusťte grafické rozhraní pomocí příkazu **strmqikm** .
2. V nabídce **Soubor databáze klíčů** klepněte na volbu **Otevřít**. Otevře se okno Otevřít.
3. Klepněte na volbu **Typ databáze klíčů** a vyberte položku **CMS** (Certificate Management System).
4. Klepněte na tlačítko **Procházet** a přejděte do adresáře, který obsahuje soubory databáze klíčů.
5. Vyberte soubor databáze klíčů, do nějž chcete přidat certifikát, tj. například `key.kdb`.
6. Klepněte na tlačítko **OK**. Otevře se okno Výzva k zadání hesla.
7. Zadejte heslo, jež jste nastavili při vytvoření databáze klíčů, a klepněte na tlačítko **OK**. Název vašeho souboru databáze klíčů se zobrazuje v poli **Název souboru**.
8. V poli **Obsah databáze klíčů** vyberte položku **Certifikáty podepsaného**.
9. Klepněte na tlačítko **Přidat**. Otevře se okno Přidat certifikát CA ze souboru.

10. Zadejte název a umístění souboru certifikátů, v němž je certifikát uložen, nebo klepněte na tlačítko **Procházet** a vyberte soubor a umístění.
11. Klepněte na tlačítko **OK**. Otevře se okno Zadat jmenovku.
12. V okně Zadat jmenovku zadejte název certifikátu.
13. Klepněte na tlačítko **OK**. Dojde k přidání certifikátu do databáze klíčů.

z příkazového řádku,

Chcete-li přidat certifikát CA do databáze klíčů, použijte jeden z následujících příkazů:

- Použití **runmqckm**:

```
runmqckm -cert -add -db filename -pw password -label label
         -file filename -format ascii
```

- Použití **runmqakm**:

```
runmqakm -cert -add -db filename -pw password -label label
         -file filename -format ascii -fips
```

kde:

-db *název souboru*
Určuje úplný název souboru databáze klíčů CMS .

-pw *heslo*
Určuje heslo pro databázi klíčů CMS .

-label *popisek*
Určuje popisek připojený k certifikátu.

-file *název_souboru*
Určuje název souboru obsahujícího certifikát.

-format *ve formátu ASCII*
Určuje formát certifikátu. Hodnota může být `ascii` pro ASCII kódované formátem Base64 nebo `binary` pro binární data DER. Výchozí hodnota: `ascii`.

-fips (fips)
určuje, že příkaz má být spuštěn v režimu FIPS. V režimu FIPS komponenta IBM Crypto for C (ICC) používá algoritmy, které byly ověřeny podle standardu FIPS 140-2. Pokud se komponenta ICC neinicializuje v režimu FIPS, příkaz **runmqakm** se nezdaří.

ALW *Export osobního certifikátu z úložiště klíčů v systému AIX, Linux, and Windows*

Chcete-li exportovat osobní certifikát, postupujte takto.

Použití produktu strmqikm

Potřebujete-li spravovat certifikáty TLS způsobem, který vyhovuje standardu FIPS, použijte příkaz **runmqakm** . **strmqikm** (iKeyman) neposkytuje volbu vyhovující standardu FIPS.

Na počítači, ze kterého chcete exportovat osobní certifikát, postupujte takto:

1. Spusťte grafické rozhraní pomocí příkazu **strmqikm** .
2. V nabídce **Soubor databáze klíčů** klepněte na volbu **Otevřít**. Otevře se okno Otevřít.
3. Klepněte na volbu **Typ databáze klíčů** a vyberte položku **CMS** (Certificate Management System).
4. Klepněte na tlačítko **Procházet** a přejděte do adresáře, který obsahuje soubory databáze klíčů.
5. Vyberte soubor databáze klíčů, ze kterého chcete exportovat certifikát, například `key.kdb`.
6. Klepněte na tlačítko **Otevřít**. Otevře se okno Výzva k zadání hesla.

7. Zadejte heslo, jež jste nastavili při vytvoření databáze klíčů, a klepněte na tlačítko **OK**. Název vašeho souboru databáze klíčů se zobrazí v poli **Název souboru** .
8. V poli **Obsah databáze klíčů** vyberte volbu **Osobní certifikáty** a vyberte certifikát, který chcete exportovat.
9. Klepněte na volbu **Exportovat/importovat**. Otevře se okno Exportovat/importovat klíč.
10. Vyberte volbu **Exportovat klíč**.
11. Vyberte **Typ souboru s klíči** certifikátu, který chcete exportovat, například **PKCS12**.
12. Zadejte název souboru a umístění, do kterého chcete exportovat certifikát, nebo klepněte na tlačítko **Procházet** a vyberte název a umístění.
13. Klepněte na tlačítko **OK**. Otevře se okno Výzva k zadání hesla. Všimněte si, že když exportujete (spíše než extrahujete) certifikát, jsou zahrnuty jak veřejné, tak soukromé části certifikátu. Proto je exportovaný soubor chráněn heslem. Když extrahujete certifikát, je zahrnuta pouze veřejná část certifikátu, takže heslo není vyžadováno.
14. Zadejte heslo do pole **Heslo** a zadejte je znovu do pole **Potvrdit heslo** .
15. Klepněte na tlačítko **OK**. Certifikát je exportován do souboru, který jste uvedli.

z příkazového řádku,

Exportujte osobní certifikát pomocí příkazu **runmqckm** nebo **runmqakm** :

```
runmqckm -cert -export -db filename -pw password -label label -type cms
        -target filename -target_pw password -target_type pkcs12
```

, nebo

```
runmqakm -cert -export -db filename -pw password -label label -type cms
        -target filename -target_pw password -target_type pkcs12
        -encryption strong | weak -fips
```

kde:

`-db filename`	je název databáze klíčů CMS včetně cesty k souboru.
`-encryption`	je síla šifrování použitá v příkazu pro export certifikátu. Hodnota může být `silný` nebo `slabý`. Výchozí hodnota je `strong`.
`-fips`	určuje, že příkaz má být spuštěn v režimu FIPS. V režimu FIPS komponenta IBM Crypto for C (ICC) používá algoritmy, které byly ověřeny podle standardu FIPS 140-2. Pokud se komponenta ICC neinicializuje v režimu FIPS, příkaz **runmqakm** se nezdaří.
`-pw password`	je heslo pro databázi klíčů CMS.
`-label label`	je jmenovka přiložená k certifikátu.
`-type cms`	je typ databáze.
`-target filename`	je úplný název cesty k cílovému souboru.
`-target_pw password`	je heslo pro šifrování certifikátu.
`-target_type pkcs12`	je typ certifikátu.

ALW *Import osobního certifikátu do úložiště klíčů v systému AIX, Linux, and Windows*

Chcete-li importovat osobní certifikát, postupujte podle této procedury.

Před importem osobního certifikátu ve formátu PKCS #12 do souboru databáze klíčů musíte nejprve přidat úplný platný řetězec vydávání certifikátů CA do souboru databáze klíčů (viz “Přidání certifikátu

CA nebo veřejné části certifikátu podepsaného držitelem do úložiště klíčů v systému AIX, Linux, and Windows" na stránce 318).

Soubory PKCS #12 by měly být po použití považovány za dočasné a měly by být odstraněny.

Použití produktu `strmqikm`

Potřebujete-li spravovat certifikáty TLS způsobem, který vyhovuje standardu FIPS, použijte příkaz **runmqakm** . Produkt **strmqikm** neposkytuje volbu vyhovující standardu FIPS.

Na počítači, do kterého chcete importovat osobní certifikát, postupujte takto:

1. Spusťte grafické rozhraní pomocí příkazu **strmqikm** .
2. V nabídce **Soubor databáze klíčů** klepněte na volbu **Otevřít**. Zobrazí se okno Otevřít.
3. Klepněte na volbu **Typ databáze klíčů** a vyberte položku **CMS** (Certificate Management System).
4. Klepněte na tlačítko **Procházet** a přejděte do adresáře, který obsahuje soubory databáze klíčů.
5. Vyberte soubor databáze klíčů, do nějž chcete přidat certifikát, tj. například `key.kdb`.
6. Klepněte na tlačítko **Otevřít**. Zobrazí se okno Výzva k zadání hesla.
7. Zadejte heslo, jež jste nastavili při vytvoření databáze klíčů, a klepněte na tlačítko **OK**. Název vašeho souboru databáze klíčů se zobrazuje v poli **Název souboru**.
8. V poli **Obsah databáze klíčů** vyberte volbu **Osobní certifikáty**.
9. Pokud se v pohledu Osobní certifikáty nacházejí certifikáty, postupujte takto:
   a. Klepněte na volbu **Exportovat/importovat**. Zobrazí se okno Exportovat/importovat klíč.
   b. Vyberte volbu **Importovat klíč**.
10. Pokud v pohledu Osobní certifikáty nejsou žádné certifikáty, klepněte na volbu **Importovat**.
11. Vyberte **Typ souboru s klíči** certifikátu, který chcete importovat, například PKCS12.
12. Zadejte název a umístění souboru certifikátů, v němž je certifikát uložen, nebo klepněte na tlačítko **Procházet** a vyberte soubor a umístění.
13. Klepněte na tlačítko **OK**. Zobrazí se okno Výzva k zadání hesla.
14. Do pole **Heslo** zadejte heslo použité při exportu certifikátu.
15. Klepněte na tlačítko **OK**. Zobrazí se okno Změnit popisky. Popisky importovaných certifikátů můžete změnit, pokud například certifikát se stejným popiskem již v cílové databázi klíčů existuje. Změna popisků certifikátů nemá žádný vliv na ověření řetězu certifikátů. Chcete-li přidružit certifikát ke konkrétnímu správci front nebo k produktu IBM MQ MQI client, produkt IBM MQ použije buď hodnotu atributu **CERTLABL** , je-li nastaven, nebo výchozí hodnotu `ibmwebspheremq` s připojeným názvem správce front nebo ID přihlášení uživatele IBM MQ MQI client , a to vše malými písmeny. Podrobnosti viz Popisky digitálních certifikátů .
16. Chcete-li změnit popisek, vyberte požadovaný popisek ze seznamu **Vybrat popisek ke změně** . Popisek se zkopíruje do vstupního pole **Zadat nový popisek** . Nahraďte text popisku textem nového popisku a klepněte na tlačítko **Použít**.
17. Text ve vstupním poli **Zadat nový popisek** se zkopíruje zpět do pole **Vybrat popisek pro změnu** a nahradí původně vybraný popisek, a tak znovu označí odpovídající certifikát.
18. Po změně všech popisků, které je třeba změnit, klepněte na tlačítko **OK**. Okno Změnit popisky se zavře a původní okno IBM Správa klíčů se znovu zobrazí s poli **Osobní certifikáty** a **Certifikáty podepsaného** aktualizovanými správně označenými certifikáty.
19. Certifikát je importován do cílové databáze klíčů.

z příkazového řádku,

Chcete-li importovat osobní certifikát pomocí produktu **runmqckm**, použijte tento příkaz:

```
runmqckm -cert -import -file filename -pw password -type pkcs12 -target filename
-target_pw password -target_type cms -label label
```

Chcete-li importovat osobní certifikát pomocí produktu **runmqakm**, použijte tento příkaz:

```
runmqakm -cert -import -file filename -pw password -type pkcs12 -target filename
-target_pw password -target_type cms -label label -fips
```

kde:

`-file filename`	je úplný název souboru obsahujícího certifikát PKCS #12 .
`-pw password`	je heslo pro certifikát PKCS #12 .
`-type pkcs12`	je typ souboru.
`-target filename`	je název cílové databáze klíčů CMS .
`-target_pw password`	je heslo pro databázi klíčů CMS.
`-target_type cms`	je typ databáze určený parametrem `-target`
`-label label`	je popisek certifikátu, který se má importovat ze zdrojové databáze klíčů.
`-new_label label`	je označení, které bude certifikát přiřazen v cílové databázi. Pokud vynecháte volbu `-new_label` , výchozí nastavení je použít stejnou volbu jako volba `-label` .
`-fips`	určuje, že příkaz má být spuštěn v režimu FIPS. V režimu FIPS komponenta IBM Crypto for C (ICC) používá algoritmy, které byly ověřeny podle standardu FIPS 140-2. Pokud se komponenta ICC neinicializuje v režimu FIPS, příkaz **runmqakm** se nezdaří.

Produkt **runmqckm** neposkytuje příkaz pro přímou změnu popisků certifikátů. Chcete-li změnit popisek certifikátu, postupujte takto:

1. Exportujte certifikát do souboru PKCS #12 pomocí příkazu **-cert -export** . Uveďte existující popisek certifikátu pro volbu `-label` .
2. Odeberte existující kopii certifikátu z původní databáze klíčů pomocí příkazu **-cert -delete** .
3. Importujte certifikát ze souboru PKCS #12 pomocí příkazu **-cert -import** . Zadejte starý popisek pro volbu `-label` a požadovaný nový popisek pro volbu `-new_label` . Certifikát bude importován zpět do databáze klíčů s požadovaným popiskem.

ALW *Import osobního certifikátu ze souboru Microsoft.pfx*

Chcete-li provést import ze souboru Microsoft.pfx na systému AIX, Linux, and Windows, postupujte takto.

Soubor .pfx může obsahovat dva certifikáty vztahující se ke stejnému klíči. Jedním z nich je osobní certifikát nebo certifikát serveru (obsahující veřejný i soukromý klíč). Druhým je certifikát CA (podepisující subjekt) (obsahující pouze veřejný klíč). Tyto certifikáty nemohou koexistovat ve stejném souboru databáze klíčů CMS , takže lze importovat pouze jeden z nich. Také "popisný název" nebo popisek je připojen pouze k certifikátu podepsaného.

Osobní certifikát je identifikován systémem generovaným jedinečným identifikátorem uživatele (UUID). V této části je zobrazen import osobního certifikátu ze souboru pfx při jeho označování popisným názvem, který byl dříve přiřazen k certifikátu CA (podepisujícího subjektu). Vydávající certifikáty CA (podepisující subjekt) by již měly být přidány do cílové databáze klíčů. Mějte na paměti, že soubory PKCS#12 by měly být po použití považovány za dočasné a měly by být odstraněny.

Chcete-li importovat osobní certifikát ze zdrojové databáze klíčů pfx, postupujte takto:

1. Spusťte grafické rozhraní pomocí příkazu **strmqikm** . Zobrazí se okno Správa klíčů IBM .
2. V nabídce **Soubor databáze klíčů** klepněte na volbu **Otevřít**. Zobrazí se okno Otevřít.
3. Vyberte typ databáze klíčů **PKCS12**.
4. **Před provedením tohoto kroku se doporučuje provést zálohu databáze pfx.** Vyberte databázi klíčů pfx, kterou chcete importovat. Klepněte na tlačítko **Otevřít**. Zobrazí se okno Výzva k zadání hesla.
5. Zadejte heslo databáze klíčů a klepněte na tlačítko **OK**. Zobrazí se okno Správa klíčů IBM . Pruh titulku zobrazuje název vybraného souboru databáze klíčů pfx, který označuje, že soubor je otevřený a připravený.
6. Ze seznamu vyberte volbu **Certifikáty podepsaného** . "popisný název" požadovaného certifikátu se zobrazí jako popisek na panelu Certifikáty podepsaného.
7. Chcete-li odebrat certifikát podepsaného, vyberte položku popisku a klepněte na tlačítko **Odstranit** . Zobrazí se okno Potvrdit.
8. Klepněte na tlačítko **Ano**. Vybraný popisek se již nezobrazuje na panelu Certifikáty podepsaného.
9. Opakujte kroky 6, 7 a 8 pro všechny certifikáty podepsaného.
10. V nabídce **Soubor databáze klíčů** klepněte na volbu **Otevřít**. Zobrazí se okno Otevřít.
11. Vyberte cílovou databázi klíče CMS , do které se importuje soubor pfx. Klepněte na tlačítko **Otevřít**. Zobrazí se okno Výzva k zadání hesla.
12. Zadejte heslo databáze klíčů a klepněte na tlačítko **OK**. Zobrazí se okno Správa klíčů IBM . Pruh titulku zobrazuje název vybraného souboru databáze klíčů, který označuje, že soubor je otevřený a připravený.
13. Ze seznamu vyberte volbu **Osobní certifikáty** .
14. Pokud se v pohledu Osobní certifikáty nacházejí certifikáty, postupujte takto:
    a. Klepněte na volbu **Exportovat/importovat klíč**. Zobrazí se okno Exportovat/importovat klíč.
    b. Vyberte volbu **Importovat** z nabídky Vybrat typ akce.
15. Pokud v pohledu Osobní certifikáty nejsou žádné certifikáty, klepněte na volbu **Importovat**.
16. Vyberte soubor PKCS12 .
17. Zadejte název souboru pfx, jak je použit v kroku 4. Klepněte na tlačítko **OK**. Zobrazí se okno Výzva k zadání hesla.
18. Zadejte stejné heslo, které jste zadali při odstranění certifikátu podepsaného. Klepněte na tlačítko **OK**.
19. Zobrazí se okno Změnit popisky (protože by měl být k dispozici pouze jeden certifikát pro import). Popisek certifikátu by měl být UUID, který má formát `xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx`.
20. Chcete-li změnit popisek, vyberte klíč UUID na panelu **Vybrat popisek pro změnu:** . Popisek bude replikován do pole **Zadat nový popisek:** . Nahraďte text popisku popisným názvem, který byl odstraněn v kroku 7, a klepněte na tlačítko **Použít**. Popisný název musí být buď hodnota atributu IBM MQ **CERTLABL** , je-li nastaven, nebo výchozí hodnota `ibmwebspheremq` s připojeným názvem správce front nebo ID přihlášení uživatele IBM MQ MQI client , vše malými písmeny. Podrobnosti viz Popisky digitálních certifikátů .
21. Klepněte na tlačítko **OK**. Okno Změnit popisky je nyní odebráno a původní okno Správa klíčů IBM se znovu zobrazí s panely Osobní certifikáty a Certifikáty podepsaného aktualizovanými správně označeným osobním certifikátem.
22. Osobní certifikát pfx je nyní importován do (cílové) databáze.

Nelze změnit popisek certifikátu pomocí **runmqckm** nebo **runmqakm**.

z příkazového řádku,

Chcete-li importovat osobní certifikát pomocí produktu **runmqckm**, použijte tento příkaz:

```
runmqckm -cert -import -file filename -pw password -type pkcs12 -target filename
-target_pw password -target_type cms -label label -pfx
```

Chcete-li importovat osobní certifikát pomocí produktu **runmqakm**, použijte tento příkaz:

```
runmqakm -cert -import -file filename -pw password -type pkcs12 -target filename
-target_pw password -target_type cms -label label -fips -pfx
```

kde:

`-file` *filename*	je úplný název souboru obsahujícího certifikát PKCS #12 .
`-pw` *password*	je heslo pro certifikát PKCS #12 .
`-type` *pkcs12*	je typ souboru.
`-target` *filename*	je název cílové databáze klíčů CMS .
`-target_pw` *password*	je heslo pro databázi klíčů CMS.
`-target_type` *cms*	je typ databáze určený parametrem `-target`
`-label` *label*	je popisek certifikátu, který se má importovat ze zdrojové databáze klíčů.
`-new_label` *label*	je označení, které bude certifikát přiřazen v cílové databázi. Pokud vynecháte volbu `-new_label` , výchozí nastavení je použít stejnou volbu jako volba `-label` .
`-fips`	určuje, že příkaz má být spuštěn v režimu FIPS. V režimu FIPS komponenta IBM Crypto for C (ICC) používá algoritmy, které byly ověřeny podle standardu FIPS 140-2. Pokud se komponenta ICC neinicializuje v režimu FIPS, příkaz **runmqakm** se nezdaří.
`-pfx`	označuje formát souboru PFX.

Produkt **runmqckm** neposkytuje příkaz pro přímou změnu popisků certifikátů. Chcete-li změnit popisek certifikátu, postupujte takto:

1. Exportujte certifikát do souboru PKCS #12 pomocí příkazu **-cert -export** . Uveďte existující popisek certifikátu pro volbu `-label` .
2. Odeberte existující kopii certifikátu z původní databáze klíčů pomocí příkazu **-cert -delete** .
3. Importujte certifikát ze souboru PKCS #12 pomocí příkazu **-cert -import** . Zadejte starý popisek pro volbu `-label` a požadovaný nový popisek pro volbu `-new_label` . Certifikát bude importován zpět do databáze klíčů s požadovaným popiskem.

ALW *Import osobního certifikátu ze souboru PKCS #7*

Nástroje **strmqikm** (iKeyman) a **runmqckm** (iKeycmd) nepodporují PKCS #7 (. p7b) souborů. Pomocí nástroje **runmqakm** naimportujte certifikáty ze souboru PKCS #7 v systému AIX, Linux, and Windows.

K přidání certifikátu CA ze souboru PKCS #7 použijte následující příkaz:

```
runmqakm -cert -add -db filename -pw password -type cms -file filename
-label label
```

`-db` *filename*	je úplný název souboru databáze klíčů CMS .
`-pw` *password*	je heslo pro databázi klíčů.
`-type` *cms*	je typ databáze klíčů.

`-file` *filename*	je název souboru PKCS #7 .
`-label` *label*	je označení, které je certifikát přiřazen v cílové databázi. První certifikát přebírá daný popisek. Všechny ostatní certifikáty, jsou-li přítomny, jsou označeny svým názvem subjektu.

Chcete-li importovat osobní certifikát ze souboru PKCS #7 , použijte následující příkaz:

```
runmqakm -cert -import -db filename -pw password -type pkcs7 -target filename
-target_pw password -target_type cms -label label -new_label label
```

`-db` *filename*	je úplný název souboru obsahujícího certifikát PKCS #7 .
`-pw` *password*	je heslo pro certifikát PKCS #7 .
`-type` *pkcs7*	je typ souboru.
`-target` *filename*	je název cílové databáze klíčů.
`-target_pw` *password*	je heslo pro cílovou databázi klíčů.
`-target_type` *cms*	je typ databáze určený parametrem `-target`
`-label` *label*	je popisek certifikátu, který má být importován.
`-new_label` *label*	je označení, které bude certifikát přiřazen v cílové databázi. Pokud vynecháte volbu `-new_label` , standardně se použije stejná volba jako volba `-label` .

ALW *Odstranění certifikátu z úložiště klíčů v systému AIX, Linux, and Windows*

Tento postup slouží k odebrání osobních certifikátů nebo certifikátů CA.

Použití produktu `strmqikm`

Potřebujete-li spravovat certifikáty TLS způsobem, který vyhovuje standardu FIPS, použijte příkaz **`runmqakm`** . **`strmqikm`** (iKeyman) neposkytuje volbu vyhovující standardu FIPS.

1. Spusťte grafické rozhraní pomocí příkazu **`strmqikm`** .
2. V nabídce **Soubor databáze klíčů** klepněte na volbu **Otevřít**. Otevře se okno Otevřít.
3. Klepněte na volbu **Typ databáze klíčů** a vyberte položku **CMS** (Certificate Management System).
4. Klepněte na tlačítko **Procházet** a přejděte do adresáře, který obsahuje soubory databáze klíčů.
5. Vyberte soubor databáze klíčů, ze kterého chcete odstranit certifikát, například `key.kdb`.
6. Klepněte na tlačítko **Otevřít**. Otevře se okno Výzva k zadání hesla.
7. Zadejte heslo, jež jste nastavili při vytvoření databáze klíčů, a klepněte na tlačítko **OK**. Název vašeho souboru databáze klíčů se zobrazí v poli **Název souboru** .
8. V rozevíracím seznamu vyberte volbu **Osobní certifikáty** nebo **Certifikáty podepsaného** .
9. Vyberte certifikát, který chcete odstranit.
10. Pokud ještě nemáte kopii certifikátu a chcete ji uložit, klepněte na volbu **Exportovat/importovat** a exportujte ji (viz “Export osobního certifikátu z úložiště klíčů v systému AIX, Linux, and Windows” na stránce 319).
11. Po výběru certifikátu klepněte na tlačítko **Odstranit**. Otevře se okno Potvrdit.
12. Klepněte na tlačítko **Ano**. Pole **Osobní certifikáty** již nezobrazuje popisek certifikátu, který jste odstranili.

z příkazového řádku,

Pomocí následujících příkazů odstraňte certifikát pomocí příkazu **`runmqckm`** nebo **`runmqakm`** :

Použití příkazu runmqckm:

```
runmqckm -cert -delete -db filename -pw password -label label
```

Použití příkazu runmqakm:

```
runmqakm -cert -delete -db filename -pw password -label label -fips
```

kde:

-db *filename*	je úplný název souboru databáze klíčů CMS .
-pw *password*	je heslo pro databázi klíčů CMS.
-label *label*	je označení připojené k osobnímu certifikátu.
-fips	určuje, že příkaz má být spuštěn v režimu FIPS. V režimu FIPS komponenta IBM Crypto for C (ICC) používá algoritmy, které byly ověřeny podle standardu FIPS 140-2. Pokud se komponenta ICC neinicializuje v režimu FIPS, příkaz **runmqakm** se nezdaří.

ALW *Generování silných hesel pro ochranu úložiště klíčů na systému AIX, Linux, and Windows*

Silná hesla pro ochranu úložiště klíčů můžete generovat pomocí příkazu **runmqakm** (GSKCapiCmd).

K vygenerování silného hesla můžete použít příkaz **runmqakm** s následujícími parametry:

```
runmqakm -random -create -length 14 -strong -fips
```

Při použití vygenerovaného hesla v parametru **-pw** následných příkazů administrace certifikátů vždy uzavřete heslo do dvojitých uvozovek. Na systémech AIX and Linux musíte také použít zpětné lomítko pro změnu významu následujících znaků, pokud se objeví v řetězci hesla:

```
! \ " '
```

Když zadáváte heslo jako odpověď na výzvu z grafického rozhraní **runmqckm**, **runmqakm** nebo **strmqikm** , pak není nutné heslo citovat nebo změnit jeho význam. Není to nutné, protože shell operačního systému v těchto případech neovlivňuje zadávání dat.

ALW *Konfigurace pro kryptografický hardware v systému AIX, Linux, and Windows*

Kryptografický hardware pro správce front nebo klienta lze konfigurovat mnoha způsoby.

Kryptografický hardware pro správce front v systému AIX, Linux, and Windows můžete konfigurovat pomocí jedné z následujících metod:

- Použijte příkaz **ALTER QMGR** MQSC s parametrem SSLCRYP , jak popisuje ALTER QMGR.
- Použijte IBM MQ Explorer ke konfiguraci šifrovacího hardwaru ve vašem systému AIX, Linux, and Windows . Další informace naleznete v nápovědě online.

Kryptografický hardware pro klienta IBM MQ na systému AIX, Linux, and Windows můžete nakonfigurovat pomocí jedné z následujících metod:

- Nastavte proměnnou prostředí **MQSSLCRYP** . Povolené hodnoty pro parametr **MQSSLCRYP** jsou stejné jako pro parametr **SSLCRYP** , jak je popsáno v části ALTER QMGR. Chcete-li nastavit tuto proměnnou prostředí, použijte jeden z těchto příkazů:

– Linux AIX Na systémech AIX and Linux:

```
export MQSSLCRYP=string
```

– Windows Na systémech Windows:

```
SET MQSSLCRYP=string
```

kde *string* představuje řetězec parametru, který se má použít ke konfiguraci šifrovacího hardwaru přítomného v systému.

Pokud použijete verzi GSK_PKCS11 parametru **SSLCRYP** , musí se popisek tokenu PKCS #11 shodovat s popiskem, se kterým jste nakonfigurovali hardware.

- Nastavte atribut **SSLCryptoHardware** v sekci SSL konfiguračního souboru IBM MQ client . Povolené hodnoty jsou stejné jako pro parametr **SSLCRYP** , jak je popsáno v tématu **ALTER QMGR**.

  Pokud použijete verzi GSK_PKCS11 parametru **SSLCRYP** , musí se popisek tokenu PKCS #11 shodovat s popiskem, se kterým jste nakonfigurovali hardware.
- Nastavte pole **CryptoHardware** struktury voleb konfigurace SSL MQSCO ve volání MQCONNX. Další informace viz Přehled pro MQSCO.

Upozornění: V 9.3.0 Při zadávání konfigurace pro kryptografický hardware prostřednictvím proměnné prostředí **MQSSLCRYP** nebo atributu **SSLCryptoHardware** byste měli heslo před uložením chránit. Další informace viz téma “IBM MQ clients , které používají kryptografický hardware” na stránce 585.

Pokud jste nakonfigurovali kryptografický hardware, který používá rozhraní PKCS #11 pomocí některé z těchto metod, musíte uložit osobní certifikát pro použití na kanálech v souboru databáze klíčů pro konfigurovaný šifrovací token. To je popsáno v tématu “Správa certifikátů na hardwaru PKCS #11” na stránce 327.

ALW *Správa certifikátů na hardwaru PKCS #11*

Digitální certifikáty můžete spravovat na šifrovacím hardwaru, který podporuje rozhraní PKCS #11 .

Informace o této úloze

Musíte vytvořit databázi klíčů pro přípravu prostředí IBM MQ , a to i v případě, že v ní nemáte v úmyslu ukládat certifikáty certifikační autority (CA), ale všechny vaše certifikáty budou uloženy na vašem šifrovacím hardwaru. Databáze klíčů je nezbytná pro odkazování správce front v poli SSLKEYR nebo pro odkazování aplikace klienta v proměnné prostředí MQSSLKEYR. Tato databáze klíčů je také vyžadována, pokud vytváříte žádost o certifikát.

Databázi klíčů vytvoříte buď pomocí příkazového řádku, nebo pomocí uživatelského rozhraní **strmqikm** (iKeyman).

Postup

Vytvořte databázi klíčů pomocí příkazového řádku.

1. Spusťte jeden z následujících příkazů:
   - Použití **runmqckm**:

     V 9.3.0 V 9.3.0

     ```
     runmqckm -keydb -create -db filename -pw password -type type -stash
     ```

- Použití **runmqakm**:

V 9.3.0 V 9.3.0

```
runmqakm -keydb -create -db filename -pw password -type type
```

kde:

-db *název souboru*
Určuje úplný název souboru databáze klíčů CMS.

-pw *heslo*
Určuje heslo pro databázi klíčů CMS V 9.3.0 V 9.3.0 nebo PKCS#12 .

V 9.3.0 V 9.3.0 **-type *typ***
Určuje typ databáze. (Pro IBM MQmusí být `cms` nebo `pkcs12`).

-stash
V 9.3.0 V 9.3.0 Volitelné. Uloží heslo databáze klíčů do souboru.

Případně vytvořte databázi klíčů pomocí uživatelského rozhraní **strmqikm** (iKeyman).

2. V systémech AIX and Linux se přihlaste jako uživatel root. V systémech Windows se přihlaste jako administrátor nebo jako člen skupiny MQM.
3. Otevřete soubor vlastností zabezpečení Java , `java.security`.
   - Na systémech AIX and Linux je soubor vlastností zabezpečení Java umístěn v podadresáři `java/jre64/jre/lib/security` instalačního adresáře IBM MQ .
   - Na systémech Windows je soubor vlastností zabezpečení Java umístěn v podadresáři `java\jre\lib\security` instalačního adresáře IBM MQ .

   Pokud již není v souboru přítomen, přidejte poskytovatele zabezpečení IBMPKCS11Impl . Například přidáním následujícího řádku:

```
security.provider.12=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl
```

4. Spusťte uživatelské rozhraní spuštěním příkazu **strmqikm** .
5. Klepněte na volbu **Soubor databáze klíčů** > **Otevřít**.
6. Klepněte na volbu **Typ databáze klíčů** a vyberte **PKCS11Direct**.
7. Do pole **Název souboru** zadejte název modulu pro správu šifrovacího hardwaru, například `PKCS11_API.so`.

   Používáte-li certifikáty nebo klíče uložené na šifrovacím hardwaru PKCS#11 , mějte na paměti, že **runmqckm** a **strmqikm** jsou 64bitové programy. Externí moduly požadované pro podporu PKCS#11 budou načteny do 64bitového procesu, proto musíte mít nainstalovanou 64bitovou knihovnu PKCS#11 pro administraci šifrovacího hardwaru. 32bitové platformy Windows a Linux x86 jsou jedinými výjimkami, protože programy **strmqikm** a **runmqckm** jsou na těchto platformách 32bitové.
8. Do pole **Umístění** zadejte cestu.
   - Na systémech AIX and Linux to může být například `/usr/lib/pksc11`.
   - V systémech Windows zadejte název knihovny. `cryptoki`, například.
9. Klepněte na tlačítko **OK**.

   Zobrazí se okno Otevřít šifrovací token.
10. Vyberte popisek tokenu šifrovacího zařízení, který chcete použít k uložení certifikátů.
11. Do pole **Heslo šifrovacího tokenu** zadejte heslo, které jste nastavili při konfiguraci šifrovacího hardwaru.
12. Pokud má váš kryptografický hardware kapacitu držet certifikáty podepsaného požadované pro přijetí nebo import osobního certifikátu, zrušte zaškrtnutí obou zaškrtávacích políček sekundární databáze klíčů a pokračujte od kroku “17” na stránce 329.

Požadujete-li sekundární databázi klíčů CMS V 9.3.0 V 9.3.0 nebo PKCS#12 k uchování certifikátů podepsaného, vyberte buď volbu **Otevřít existující sekundární soubor databáze klíčů** , nebo volbu **Vytvořit nový sekundární soubor databáze klíčů**.

13. Do pole **Název souboru** zadejte název souboru.

    Toto pole již obsahuje text `key.kdb`. Pokud je název vašeho kmene `key`, ponechte toto pole nezměněné. Pokud jste zadali jiný název stonku, nahraďte `key` svým názvem stonku.

14. Do pole **Umístění** zadejte cestu. Příklad:

    - Pro správce front: `/var/mqm/qmgrs/QM1/ssl`
    - Pro IBM MQ MQI client: `/var/mqm/ssl`

15. Klepněte na tlačítko **OK**.

    Zobrazí se okno Výzva k zadání hesla.

16. Zadejte heslo.

    Pokud jste v kroku “12” na stránce 328vybrali volbu **Otevřít existující sekundární soubor databáze klíčů** , zadejte heslo do pole **Heslo** .

    Pokud jste v kroku “12” na stránce 328vybrali volbu **Vytvořit nový sekundární soubor databáze klíčů** , postupujte takto:

    a) Zadejte heslo do pole **Heslo** a zadejte je znovu do pole **Potvrdit heslo** .

    b) V 9.3.0 V 9.3.0
    Chcete-li uložit heslo do souboru, vyberte volbu **Ukrýt heslo do souboru**. Pokud heslo neschováte, musíte zadat heslo databáze klíčů do správce front pomocí atributu KEYRPWD nebo do souboru IBM MQ MQI client pomocí jedné z metod popsaných v části “Zadání hesla úložiště klíčů pro IBM MQ MQI client on AIX, Linux, and Windows” na stránce 304.

    c) V 9.3.0 V 9.3.0
    Klepněte na tlačítko **OK**.

    Pokud jste se rozhodli uložit heslo do souboru, otevře se okno s potvrzením, že heslo je v souboru `key.sth` (pokud jste neuvedli jiný kmenový název).

17. Klepněte na tlačítko **OK**.

    Zobrazí se rámec obsahu databáze klíčů.

ALW *Vyžádání osobního certifikátu pro hardware PKCS #11*

Tento postup použijte buď pro správce front, nebo pro IBM MQ MQI client , chcete-li požádat o osobní certifikát pro váš šifrovací hardware.

Informace o této úloze

Tato úloha popisuje, jak použít uživatelské rozhraní **strmqikm** k vyžádání osobního certifikátu. Pokud používáte rozhraní příkazového řádku, viz “z příkazového řádku,” na stránce 312.

Poznámka: Produkt IBM MQ nepodporuje algoritmy SHA-3 nebo SHA-5 . Můžete použít názvy algoritmů digitálního podpisu SHA384WithRSA a SHA512WithRSA , protože oba algoritmy jsou členy řady SHA-2 .

Deprecated Názvy algoritmů digitálního podpisu SHA3WithRSA a SHA5WithRSA jsou zamítnuty, protože se jedná o zkrácenou formu SHA384WithRSA a SHA512WithRSA .

Postup

Chcete-li požádat o osobní certifikát z uživatelského rozhraní produktu **strmqikm** (iKeyman), postupujte takto:

1. Dokončete kroky pro práci s kryptografickým hardwarem. Viz “Správa certifikátů na hardwaru PKCS #11” na stránce 327.
2. V nabídce **Vytvořit** klepněte na volbu **Nová žádost o certifikát**.

Otevře se okno Vytvořit nový klíč a žádost o certifikát.

3. Do pole **Popisek klíče** zadejte popisek certifikátu.

   Popisek je buď hodnota atributu **CERTLABL** , je-li nastaven, nebo výchozí hodnota `ibmwebspheremq` s připojeným jménem správce front nebo ID uživatele pro přihlášení IBM MQ MQI client , vše malými písmeny. Podrobnosti viz Popisky digitálních certifikátů .
4. Vyberte **Velikost klíče** a **Podpisový algoritmus** , který požadujete.
5. Zadejte hodnoty pro **Obecný název** a **Organizaci**a vyberte **Země**. Pro zbývající volitelná pole buď přijměte výchozí hodnoty, nebo zadejte nebo vyberte nové hodnoty.

   Všimněte si, že do pole **Organizační jednotka** můžete zadat pouze jeden název. Další informace o těchto polích viz “Rozlišující názvy” na stránce 14.
6. Do pole **Zadejte název souboru, do kterého se má uložit žádost o certifikát** buď přijměte předvolbu `certreq.arm`, nebo zadejte novou hodnotu s úplnou cestou.
7. Klepněte na tlačítko **OK**.

   Otevře se okno Potvrzení.
8. Klepněte na tlačítko **OK**.

   Seznam **Požadavky na osobní certifikát** zobrazuje popisek nové žádosti o osobní certifikát, kterou jste vytvořili. Žádost o certifikát je uložena v souboru, který jste vybrali v kroku “6” na stránce 330.
9. Požádejte o nový osobní certifikát buď odesláním souboru certifikační autoritě (CA), nebo zkopírováním souboru do formuláře požadavku na webu certifikační autority.

ALW *Příjem osobního certifikátu do hardwaru PKCS #11*

Tento postup použijte buď pro správce front, nebo pro server IBM MQ MQI client , abyste obdrželi osobní certifikát pro váš šifrovací hardware.

Než začnete

Přidejte certifikát certifikační autority, která podepsala osobní certifikát. Přidejte jej buď do šifrovacího hardwaru, nebo do sekundární databáze klíčů CMS . Toto proveďte před přijetím podepsaného certifikátu do šifrovacího hardwaru. Chcete-li přidat certifikát CA do svazku klíčů, postupujte podle pokynů v části “Přidání certifikátu CA nebo veřejné části certifikátu podepsaného držitelem do úložiště klíčů v systému AIX, Linux, and Windows” na stránce 318.

Procedura

- Chcete-li přijmout osobní certifikát pomocí uživatelského rozhraní **strmqikm** (iKeyman), postupujte takto:
  a) Dokončete kroky pro práci s kryptografickým hardwarem. Viz “Správa certifikátů na hardwaru PKCS #11” na stránce 327.
  b) Klepněte na tlačítko **Přijmout**. Otevře se okno Přijmout certifikát ze souboru.
  c) Zadejte název souboru certifikátů a umístění nového osobního certifikátu nebo klepněte na tlačítko **Procházet** a vyberte název a umístění.
  d) Klepněte na tlačítko **OK**. Pokud již máte osobní certifikát v databázi klíčů, otevře se okno s dotazem, zda chcete nastavit klíč, který přidáváte jako výchozí klíč v databázi.
  e) Klepněte na volbu **Ano** nebo **Ne**. Otevře se okno Zadat jmenovku.
  f) Klepněte na tlačítko **OK**. Seznam **Osobní certifikáty** zobrazuje popisek nového osobního certifikátu, který jste přidali. Tento popisek je vytvořen přidáním popisku šifrovacího tokenu před vámi zadaný popisek.
- Chcete-li přijmout osobní certifikát pomocí příkazu **runmqakm** (GSKCapiCmd), postupujte takto:
  a) Otevřete příkazové okno, které je nakonfigurováno pro vaše prostředí.
  b) Přijměte osobní certifikát pomocí příkazu **runmqakm** (GSKCapiCmd):

```
runmqakm -cert -receive -file filename -crypto module_name
```

```
          -tokenlabel hardware_token -pw hardware_password
          -format cert_format -fips
          -secondaryDB filename -secondaryDBpw password
```

kde:

-file *název_souboru*
Určuje úplný název souboru obsahujícího osobní certifikát.

-crypto *název_modulu*
Určuje úplný název knihovny PKCS #11 dodávané s šifrovacím hardwarem.

-tokenlabel *token_token*
Určuje popisek tokenu šifrovacího zařízení PKCS #11 .

-pw *heslo_hardware_password*
Určuje heslo pro přístup k kryptografickému hardwaru.

-format *cert_format*
Určuje formát certifikátu. Hodnota může být `ascii` pro ASCII kódované formátem Base64 nebo `binary` pro binární data DER. Předvolba je ASCII.

-fips (fips)
určuje, že příkaz má být spuštěn v režimu FIPS. V režimu FIPS komponenta IBM Crypto for C (ICC) používá algoritmy, které jsou ověřeny podle standardu FIPS 140-2. Pokud se komponenta ICC neinicializuje v režimu FIPS, příkaz **runmqakm** se nezdaří.

-secondaryDB *název souboru*
Určuje úplný název souboru databáze klíčů CMS .

-secondaryDBpw *heslo*
Určuje heslo pro databázi klíčů CMS .

MQ Appliance Práce se zabezpečením SSL/TLS v systému IBM MQ Appliance

Produkt IBM MQ Appliance má podporu protokolu TLS (Transport Layer Security).

IBM MQ Appliance má různé příkazy pro správu certifikátů. Podrobné informace o správě certifikátů naleznete v dokumentaci IBM MQ Appliance , Správa certifikátů TLS .

z/OS Práce se zabezpečením SSL/TLS v systému z/OS

Tyto informace popisují nastavení a práci se zabezpečením TLS (Transport Layer Security) v systému z/OS.

Každé téma obsahuje příklady provedení jednotlivých úloh pomocí RACF. Podobné úlohy můžete provádět pomocí jiných externích správců zabezpečení.

V systému z/OSmusíte také nastavit počet podúloh serveru, které každý správce front používá pro zpracování volání TLS, jak je popsáno v tématu “Nastavení parametru SSLTASKS na z/OS” na stránce 332.

z/OS Podpora TLS je nedílnou součástí operačního systému a je známa jako *System SSL*. Zabezpečení SSL systému je součástí základního prvku kryptografických služeb produktu z/OS. Základní členové šifrovacích služeb jsou instalováni v adresáři *pdsname*. rozdělená datová sada SIEALNKE (PDS). Při instalaci zabezpečení SSL systému se ujistěte, že jste vybrali příslušné volby pro zadání požadovaných CipherSpecs .

Potřebujete-li obnovit certifikát podepsaný svým držitelem, další informace viz Kroky pro obnovení certifikátu podepsaného svým držitelem v RACF .

z/OS *Další požadavky na ID uživatele pro TLS na systému z/OS*

Tyto informace popisují další požadavky, které vaše ID uživatele potřebuje k nastavení a práci s protokolem TLS v systému z/OS.

Ujistěte se, že máte ve svém systému všechny odpovídající aktualizace s vysokým dopadem nebo Pervasivní (HIPER).

Pokud je úložiště klíčů vlastněno ID uživatele CHINIT, toto ID uživatele potřebuje přístup pro čtení k IRR IRR.DIGTCERT.LISTRING ve třídě FACILITY a jinak aktualizujte přístup a přístup pro čtení k IRR IRR.DIGTCERT.LIST . Podle potřeby udělte přístup pomocí příkazu PERMIT s příkazem ACCESS (UPDATE) nebo ACCESS (READ).

Ujistěte se, že jste nastavili následující předpoklady:

- ID uživatele *ssidCHIN* je v produktu RACFdefinováno správně a ID uživatele *ssidCHIN* má odpovídající přístup k následujícím profilům:
  - IRR.DIGTCERT.LIST
  - IRR.DIGTCERT.LISTRING

  Tyto proměnné jsou definovány ve třídě RACF FACILITY.
- ID uživatele *ssidCHIN* je vlastníkem svazku klíčů.
- Osobní certifikát správce front, pokud je vytvořen příkazem RACDCERT, je vytvořen s ID uživatele typu certifikátu, které je stejné jako ID uživatele *ssidCHIN* .
- Iniciátor kanálu je recyklován nebo je vydán příkaz **REFRESH SECURITY TYPE(SSL)** , který vybere všechny změny, které provedete v svazku klíčů.
- Procedura IBM MQ Channel Initiator má přístup k běhové knihovně SSL systému *pdsname*.SIEALNKE prostřednictvím seznamu odkazů, LPA nebo příkazu STEPLIB DD. Tato knihovna musí mít autorizaci APF.
- ID uživatele, pod jehož oprávněním je spuštěn inicializátor kanálu, je nakonfigurováno pro použití z/OS UNIX System Services (z/OS UNIX), jak je popsáno v dokumentaci z/OS UNIX System Services Plánování .

  Uživatelé, kteří nechtějí, aby inicializátor kanálu vyvolal z/OS UNIX pomocí segmentu guest/default UID a OMVS, potřebují pouze modelovat nový segment OMVS založený na výchozím segmentu, protože iniciátor kanálu nevyžaduje žádná speciální oprávnění a nespouští se v rámci produktu UNIX jako superuživatel.

  Některé ukázkové příkazy viz “Udělení správných přístupových práv inicializátoru kanálu v systému z/OS” na stránce 334 .

z/OS *Nastavení parametru SSLTASKS na z/OS*

Pomocí příkazu ALTER QMGR nastavte počet dílčích úloh serveru pro zpracování volání TLS.

Chcete-li používat kanály TLS, pomocí příkazu ALTER QMGR nastavte parametr SSLTASKS tak, aby obsahoval alespoň dvě dílčí úlohy serveru. Příklad:

```
ALTER QMGR SSLTASKS(5)
```

Chcete-li se vyhnout problémům s přidělením úložiště, nenastavujte atribut SSLTASKS na hodnotu větší než osm v prostředí, kde není kontrola seznamu odvolaných certifikátů (CRL).

Pokud je použita kontrola CRL, je SSLTASK zadržen příslušným kanálem po dobu trvání této kontroly. Může se jednat o významnou uplynulou dobu při kontaktování příslušného serveru LDAP, protože každý SSLTASK je řídicí blok úlohy z/OS .

Musíte restartovat inicializátor kanálu, pokud změníte hodnotu atributu SSLTASKS.

z/OS *Nastavení úložiště klíčů v systému z/OS*

Nastavte úložiště klíčů na obou koncích připojení. Přidružte každé úložiště klíčů k příslušnému správci front.

Připojení TLS vyžaduje na každém konci připojení *úložiště klíčů* . Každý správce front musí mít přístup k úložišti klíčů. Pomocí parametru SSLKEYR v příkazu ALTER QMGR přidružte úložiště klíčů ke správci front. Další informace viz “Úložiště klíčů SSL/TLS” na stránce 25.

V systému z/OSjsou digitální certifikáty uloženy v *svazku klíčů* , který je spravován externím správcem zabezpečení (ESM). Tyto digitální certifikáty mají jmenovky, které přidružují certifikát ke správci front. TLS

používá tyto certifikáty pro účely ověření. Všechny následující příklady používají příkazy RACF . Pro jiné programy ESM existují ekvivalentní příkazy.

V systému z/OSpoužívá systém IBM MQ buď hodnotu atributu **CERTLABL** , je-li nastaven, nebo výchozí hodnotu `ibmWebSphereMQ` s připojeným názvem správce front. Podrobnosti viz Popisky digitálních certifikátů .

Název úložiště klíčů pro správce front je název svazku klíčů ve vaší databázi RACF . Název svazku klíčů můžete zadat buď před, nebo po vytvoření svazku klíčů.

Chcete-li vytvořit nový svazek klíčů pro správce front, postupujte takto:

1. Ujistěte se, že máte odpovídající oprávnění k zadání příkazu RACDCERT (další podrobnosti viz Řízení použití příkazu RACDCERT).
2. Spusťte následující příkaz:

   ```
   RACDCERT ID( userid1 ) ADDRING( ring-name )
   ```

   kde:

   - *userid1* je ID uživatele adresního prostoru inicializátoru kanálu nebo ID uživatele, který bude vlastnit svazek klíčů (pokud je svazek klíčů sdílený).
   - *ring-name* je název, který chcete dát vašemu svazku klíčů. Délka tohoto názvu může být až 237 znaků. V tomto jménu se rozlišují velká a malá písmena. Zadejte *ring-name* velkými písmeny, abyste se vyhnuli problémům.

z/OS *Zpřístupnění certifikátů CA pro správce front v systému z/OS*

Po vytvoření svazku klíčů k němu připojte všechny příslušné certifikáty CA.

Pokud máte certifikát CA v datové sadě, musíte jej nejprve přidat do databáze RACF pomocí následujícího příkazu:

```
RACDCERT ID( userid1 ) ADD( input-data-set-name ) WITHLABEL( 'My CA' )
```

Poté pomocí následujícího příkazu připojte certifikát CA pro produkt My CA ke svazku klíčů:

```
RACDCERT ID(userid1)
CONNECT(CERTAUTH LABEL('My CA') RING(ring-name) USAGE(CERTAUTH))
```

kde *userid1* je buď ID uživatele inicializátoru kanálu, nebo vlastník svazku sdílených klíčů.

Další informace o certifikátech CA viz “digitální certifikáty” na stránce 13.

z/OS *Vyhledání úložiště klíčů pro správce front v systému z/OS*

Pomocí této procedury získáte umístění svazku klíčů správce front.

1. Zobrazte atributy správce front pomocí jednoho z následujících příkazů MQSC:

   ```
   DISPLAY QMGR ALL
   DISPLAY QMGR SSLKEYR
   ```

2. Zkontrolujte výstup příkazu pro umístění svazku klíčů.

z/OS *Určení umístění úložiště klíčů pro správce front v systému z/OS*

Chcete-li určit umístění svazku klíčů správce front, nastavte pomocí příkazu ALTER QMGR MQSC atribut úložiště klíčů správce front.

Příklad:

```
ALTER QMGR SSLKEYR(CSQ1RING)
```

pokud je svazek klíčů vlastněn adresním prostorem inicializátoru kanálu, nebo:

```
ALTER QMGR SSLKEYR(userid1/CSQ1RING)
```

pokud se jedná o sdílený svazek klíčů, kde *userid1* je ID uživatele, který vlastní svazek klíčů.

z/OS *Udělení správných přístupových práv inicializátoru kanálu v systému z/OS*

Inicializátor kanálu (CHINIT) potřebuje přístup k úložišti klíčů a k určitým profilům zabezpečení.

Udělení přístupu CHINIT pro čtení úložiště klíčů

Pokud je úložiště klíčů vlastněno ID uživatele CHINIT, toto ID uživatele potřebuje přístup pro čtení k IRR IRR.DIGTCERT.LISTRING ve třídě FACILITY a jinak aktualizujte přístup a přístup pro čtení k IRR IRR.DIGTCERT.LIST . Udělte přístup pomocí příkazu PERMIT s parametrem ACCESS (UPDATE) nebo ACCESS (READ) podle potřeby:

```
PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID( userid ) ACCESS(UPDATE)
PERMIT IRR.DIGTCERT.LIST CLASS(FACILITY) ID( userid ) ACCESS(READ)
```

kde *userid* je ID uživatele adresního prostoru inicializátoru kanálu.

Udělení přístupu pro čtení CHINIT k příslušným profilům CSF*

Chcete-li použít hardwarovou podporu poskytovanou prostřednictvím ICSF (Integrated Cryptographic Service Facility), ujistěte se, že vaše ID uživatele CHINIT má přístup pro čtení k příslušným profilům CSF* ve třídě CSFSERV pomocí následujícího příkazu:

```
PERMIT csf-resource CLASS(CSFSERV) ID( userid ) ACCESS(READ)
```

kde *csf-resource* je název profilu CSF* a *userid* je ID uživatele adresního prostoru inicializátoru kanálu.

Zopakujte tento příkaz pro každý z následujících profilů CSF*:

- CSFDSG
- CSFDSV
- CSFPKD
- CSFPKE
- CSFPKI

Vaše ID uživatele CHINIT může také vyžadovat přístup pro čtení k jiným profilům CSF*. Pokud například používáte specifikaci šifrování ECDHE_RSA_AES_256_GCM_SHA384 , vaše ID uživatele CHINIT také potřebuje přístup pro čtení k následujícím profilům CSF*:

- CSF1DVK
- CSF1GAV
- CSF1GKP
- CSF1SKE
- CSF1TRC
- CSF1TRD

Další informace viz RACF Požadavky na prostředky CSFSERV.

Pokud jsou vaše klíče certifikátů uloženy v ICSF a vaše instalace zavedla řízení přístupu ke klíčům uloženým v ICSF, ujistěte se, že vaše ID uživatele CHINIT má přístup pro čtení k profilu ve třídě CSFKEYS pomocí následujícího příkazu:

```
PERMIT IRR.DIGTCERT. userid.* CLASS(CSFKEYS) ID( userid ) ACCESS(READ)
```

kde *userid* je ID uživatele adresního prostoru inicializátoru kanálu.

Použití ICSF (Integrated Cryptographic Service Facility)

Inicializátor kanálu může použít ICSF ke generování náhodného čísla při zavedení algoritmu ochrany hesla pro zamlžení hesel proudících přes kanály klienta, pokud se nepoužívá TLS.

Další informace viz “Použití ICSF (Integrated Cryptographic Service Facility)” na stránce 264

z/OS *Když změny certifikátů nebo úložiště klíčů vstoupí v platnost v systému z/OS*

Změny vstoupí v platnost při spuštění inicializátoru kanálu nebo při aktualizaci úložiště.

Konkrétně změny certifikátů ve svazku klíčů a v atributu úložiště klíčů nabývají platnosti při jedné z následujících událostí:

- Při spuštění nebo restartování inicializátoru kanálu.
- Při zadání příkazu REFRESH SECURITY TYPE (SSL) k aktualizaci obsahu úložiště klíčů.

z/OS *Vytvoření osobního certifikátu podepsaného (svým) držitelem v systému z/OS*

Pomocí této procedury vytvoříte osobní certifikát podepsaný svým držitelem.

1. Vygenerujte certifikát a dvojici veřejného a soukromého klíče pomocí následujícího příkazu:

```
RACDCERT ID(userid2) GENCERT
SUBJECTSDN(CN('common-name')
           T('title')
           OU('organizational-unit')
           O('organization')
           L('locality')
           SP('state-or-province')
           C('country'))
WITHLABEL('label-name')
```

2. Připojte certifikát ke svazku klíčů pomocí následujícího příkazu:

```
RACDCERT ID(userid1)
CONNECT(ID(userid2) LABEL('label-name') RING(ring-name) USAGE(PERSONAL))
```

kde:

- *userid1* je ID uživatele adresního prostoru inicializátoru kanálu nebo vlastníka svazku sdílených klíčů.
- *userid2* je ID uživatele přidružené k certifikátu a musí být ID uživatele adresního prostoru inicializátoru kanálu.

  userid1 a *userid2* mohou být stejné ID.
- *ring-name* je název, který jste dali svazku klíčů v souboru “Nastavení úložiště klíčů v systému z/OS” na stránce 332.
- *label-name* musí být buď hodnota atributu IBM MQ **CERTLABL** , je-li nastaven, nebo výchozí hodnota `ibmWebSphereMQ` s připojeným názvem správce front. Podrobnosti viz Popisky digitálních certifikátů .

z/OS *Vyžádání osobního certifikátu na z/OS*

Zažádat o osobní certifikát pomocí RACF.

Chcete-li požádat o osobní certifikát, použijte RACF takto:

1. Vytvořte osobní certifikát podepsaný svým držitelem, jak je uvedeno v části “Vytvoření osobního certifikátu podepsaného (svým) držitelem v systému z/OS” na stránce 335. Tento certifikát poskytuje požadavek s hodnotami atributů pro rozlišující název.
2. Vytvořte žádost o certifikát PKCS #10 Base64-encoded zapsanou do datové sady pomocí následujícího příkazu:

   ```
   RACDCERT ID(userid2) GENREQ(LABEL(' label_name ')) DSN(' output_data_set_name ')
   ```

   kde:

   - *userid2* je ID uživatele přidružené k certifikátu a musí být ID uživatele adresního prostoru inicializátoru kanálu.
   - *label_name* je popisek použitý při vytváření certifikátu podepsaného (svým) držitelem

   Podrobnosti viz “Digitální štítky certifikátů, pochopení požadavků” na stránce 26.
3. Odešlete datovou sadu certifikační autoritě (CA) a požádejte o nový osobní certifikát.
4. Když vám certifikační autorita vrátí podepsaný certifikát, přidejte jej zpět do databáze RACF s použitím původního popisku, jak je popsáno v tématu “Přidání osobních certifikátů do úložiště klíčů v systému z/OS” na stránce 337.

z/OS *Vytvoření RACF podepsaného osobního certifikátu*

Produkt RACF může fungovat jako certifikační autorita a vydávat vlastní certifikát certifikační autority.

Tato sekce používá termín *certifikát podepsaného* k označení certifikátu CA vydaného produktem RACF.

Soukromý klíč pro certifikát podepsaného musí být v databázi RACF před provedením následujícího postupu:

1. Pomocí následujícího příkazu vygenerujte osobní certifikát podepsaný produktem RACFs použitím certifikátu podepsaného obsaženého v databázi RACF :

   ```
   RACDCERT ID(userid2) GENCERT
   SUBJECTSDN(CN('common-name')
              T('title')
              OU('organizational-unit')
              O('organization')
              L('locality')
              SP('state-or-province')
              C('country'))
   WITHLABEL('label-name')
   SIGNWITH(CERTAUTH LABEL('signer-label'))
   ```

2. Připojte certifikát ke svazku klíčů pomocí následujícího příkazu:

   ```
   RACDCERT ID(userid1)
   CONNECT(ID(userid2) LABEL('label-name') RING(ring-name) USAGE(PERSONAL))
   ```

kde:

- *userid1* je ID uživatele adresního prostoru inicializátoru kanálu nebo vlastníka svazku sdílených klíčů.
- *userid2* je ID uživatele přidružené k certifikátu a musí být ID uživatele adresního prostoru inicializátoru kanálu.

  userid1 a *userid2* mohou být stejné ID.
- *ring-name* je název, který jste dali svazku klíčů v souboru “Nastavení úložiště klíčů v systému z/OS” na stránce 332.

- *label-name* musí být buď hodnota atributu IBM MQ **CERTLABL** , je-li nastaven, nebo výchozí hodnota `ibmWebSphereMQ` s připojeným názvem správce front nebo skupiny sdílení front. Podrobnosti viz Popisky digitálních certifikátů .
- *jmenovka podepisujícího subjektu* je jmenovka vašeho vlastního certifikátu podepisujícího subjektu.

z/OS *Přidání osobních certifikátů do úložiště klíčů v systému z/OS*

Pomocí této procedury přidáte nebo naimportujete osobní certifikát do svazku klíčů.

Poté, co vám certifikační autorita odešle nový osobní certifikát, přidejte jej do svazku klíčů pomocí následujícího postupu:

1. Přidejte certifikát do databáze RACF pomocí následujícího příkazu:

```
RACDCERT ID( userid2 ) ADD( input-data-set-name ) WITHLABEL(' label-name ')
```

2. Připojte certifikát ke svazku klíčů pomocí následujícího příkazu:

```
RACDCERT ID( userid1 )
CONNECT(ID( userid2 ) LABEL(' label-name ') RING( ring-name ) USAGE(PERSONAL))
```

kde:

- *userid1* je ID uživatele adresního prostoru inicializátoru kanálu nebo vlastníka svazku sdílených klíčů.
- *userid2* je ID uživatele přidružené k certifikátu a musí být ID uživatele adresního prostoru inicializátoru kanálu.
- *ring-name* je název, který jste dali svazku klíčů v souboru “Nastavení úložiště klíčů v systému z/OS” na stránce 332.
- *input-data-set-name* je název datové sady obsahující podepsaný certifikát CA. Datová sada musí být katalogizována a nesmí být PDS nebo členem PDS. Formát záznamu (RECFM) očekávaný RACDCERT je VB. RACDCERT dynamicky přiděluje a otevírá datovou sadu a čte z ní certifikát jako binární data.
- *label-name* je název popisku, který byl použit při vytváření původního požadavku. Musí se jednat buď o hodnotu atributu IBM MQ **CERTLABL** , je-li nastaven, nebo o výchozí hodnotu `ibmWebSphereMQ` s připojeným názvem správce front nebo skupiny sdílení front. Podrobnosti viz Popisky digitálních certifikátů .

z/OS *Export osobního certifikátu z úložiště klíčů v systému z/OS*

Exportujte certifikát pomocí příkazu RACDCERT.

V systému, ze kterého chcete exportovat certifikát, použijte následující příkaz:

```
RACDCERT ID(userid2) EXPORT(LABEL('label-name'))
DSN(output-data-set-name) FORMAT(CERTB64)
```

kde:

- *userid2* je ID uživatele, pod kterým byl certifikát přidán do svazku klíčů.
- *název-jmenovky* je jmenovka certifikátu, který chcete extrahovat.
- *output-data-set-name* je datová sada, do které je certifikát umístěn.
- CERTB64 je certifikát kódovaný pomocí DER X.509 , který je ve formátu Base64 . Můžete zvolit alternativní formát, například:

  CERTDER
  DER zakódovaný X.509 certifikát v binárním formátu

  PKCS12B64
  Certifikát PKCS #12 ve formátu Base64

PKCS12DER
Certifikát PKCS #12 v binárním formátu

z/OS *Odstranění osobního certifikátu z úložiště klíčů v systému z/OS*

Odstraňte osobní certifikát pomocí příkazu RACDCERT.

Před odstraněním osobního certifikátu můžete uložit jeho kopii. Chcete-li zkopírovat osobní certifikát do datové sady před jeho odstraněním, postupujte podle pokynů v části "Export osobního certifikátu z úložiště klíčů v systému z/OS" na stránce 337. Poté pomocí následujícího příkazu odstraňte svůj osobní certifikát:

```
RACDCERT ID( userid2 ) DELETE(LABEL(' label-name '))
```

kde:

- *userid2* je ID uživatele, pod kterým byl certifikát přidán do svazku klíčů.
- *label-name* je název certifikátu, který chcete odstranit.

z/OS *Přejmenování osobního certifikátu v úložišti klíčů na z/OS*

Přejmenujte certifikát pomocí příkazu RACDCERT.

Pokud nechcete, aby byl nalezen certifikát se specifickým popiskem, ale nechcete jej odstranit, můžete jej dočasně přejmenovat pomocí následujícího příkazu:

```
RACDCERT ID( userid2 ) LABEL(' label-name ') NEWLABEL(' new-label-name ')
```

kde:

- *userid2* je ID uživatele, pod kterým byl certifikát přidán do svazku klíčů.
- *label-name* je název certifikátu, který chcete přejmenovat.
- *new-label-name* je nový název certifikátu.

To může být užitečné při testování ověření klienta TLS.

z/OS *Přidružení ID uživatele k digitálnímu certifikátu v systému z/OS*

Produkt IBM MQ může použít ID uživatele přidružené k certifikátu RACF jako ID uživatele kanálu. Přidružte ID uživatele k certifikátu jeho instalací pod tímto ID uživatele nebo pomocí filtru názvů certifikátů.

Metoda popsaná v tomto tématu je alternativou k metodě nezávislé na platformě pro přidružení ID uživatele k digitálnímu certifikátu, který používá záznamy ověření kanálu. Další informace o záznamech ověřování kanálu viz "Záznamy ověření kanálu" na stránce 51.

Když entita na jednom konci kanálu TLS obdrží certifikát ze vzdáleného připojení, entita se zeptá RACF , zda je k tomuto certifikátu přidruženo ID uživatele. Entita používá toto ID uživatele jako ID uživatele kanálu. Pokud k certifikátu není přidruženo žádné ID uživatele, entita použije ID uživatele, pod kterým je spuštěn inicializátor kanálu.

Přidružte ID uživatele k certifikátu jedním z následujících způsobů:

- Nainstalujte tento certifikát do databáze RACF pod ID uživatele, ke kterému jej chcete přidružit, jak je popsáno v tématu "Přidání osobních certifikátů do úložiště klíčů v systému z/OS" na stránce 337.
- Pomocí filtru CNF (Certificate Name Filter) namapujte rozlišující název subjektu nebo vydavatele certifikátu na ID uživatele, jak je popsáno v tématu "Nastavení filtru názvů certifikátů na systému z/OS" na stránce 338.

z/OS *Nastavení filtru názvů certifikátů na systému z/OS*

Pomocí příkazu RACDCERT definujte filtr názvů certifikátů (CNF), který mapuje rozlišující název na ID uživatele.

Chcete-li nastavit CNF, postupujte takto.

1. Povolte funkce CNF pomocí následujícího příkazu. K tomu potřebujete oprávnění k aktualizaci třídy DIGTNMAP.

```
SETROPTS CLASSACT(DIGTNMAP) RACLIST(DIGTNMAP)
```

2. Definujte CNF. Příklad:

```
RACDCERT ID(USER1) MAP WITHLABEL('filter1') TRUST
SDNFILTER('O=IBM.C=UK') IDNFILTER('O=ExampleCA.L=Internet')
```

   kde USER1 je ID uživatele, které se má použít, když:

   - Rozlišující název předmětu má organizaci `IBM` a zemi UK.
   - DN vydavatele má organizaci `ExampleCA` a lokalita `Internet`.

3. Aktualizovat mapování CNF:

```
SETROPTS RACLIST(DIGTNMAP) REFRESH
```

Poznámka:

1. Pokud je skutečný certifikát uložen v databázi RACF , použije se ID uživatele, pod kterým je nainstalován, namísto ID uživatele přidruženého k libovolnému CNF. Pokud není certifikát uložen v databázi RACF , použije se ID uživatele přidružené k nejspecifičtějšímu odpovídajícímu CNF. Shody rozlišujícího názvu subjektu jsou považovány za specifičtější než shody rozlišujícího názvu vydavatele.
2. Změny CNF se nepoužijí, dokud neobnovíte mapování CNF.
3. DN se shoduje s filtrem DN v CNF pouze v případě, že je filtr DN identický s *nejméně významnou částí* DN. Nejméně významná část DN se skládá z atributů, které jsou obvykle uvedeny na pravém konci DN, ale které se objevují na začátku certifikátu.

   Zvažte například SDNFILTER `'O=IBM.C=UK'`. Rozlišující název předmětu `'CN=QM1.O=IBM.C=UK'` odpovídá tomuto filtru, ale rozlišující název předmětu `'CN=QM1.O=IBM.L=Hursley.C=UK'` neodpovídá tomuto filtru.

   Nejméně významná část některých certifikátů může obsahovat pole, která neodpovídají filtru DN. Zvažte vyloučení těchto certifikátů zadáním vzoru DN ve vzoru SSLPEER v příkazu DEFINE CHANNEL.
4. Je-li nejspecifičtější vyhovující CNF definována pro RACF jako NOTRUST, entita použije ID uživatele, pod kterým je spuštěn inicializátor kanálu.
5. RACF používá jako oddělovač znak `'.'` . IBM MQ používá buď čárku, nebo středník.

Můžete definovat CNFs, abyste zajistili, že entita nikdy nenastaví ID uživatele kanálu na výchozí hodnotu, což je ID uživatele, pod kterým je spuštěn inicializátor kanálu. Pro každý certifikát CA v svazku klíčů přidruženém k entitě definujte CNF s IDNFILTER, který přesně odpovídá DN subjektu daného certifikátu CA. To zajistí, že všechny certifikáty, které může entita použít, budou odpovídat alespoň jednomu z těchto CNF. Důvodem je, že všechny tyto certifikáty musí být buď připojeny ke svazku klíčů přidruženému k entitě, nebo musí být vydány certifikační autoritou, pro kterou je certifikát připojen ke svazku klíčů přidruženému k entitě.

Další informace o příkazech, které používáte k manipulaci s CNF, naleznete v příručce *z/OS Security Server RACF Security Administrator's Guide* .

z/OS *Definování kanálu odesilatele a přenosové fronty v systému QMA v systému z/OS*

Pomocí příkazů **DEFINE CHANNEL** a **DEFINE QLOCAL** nastavte požadované objekty.

Postup

V systému QMA zadejte příkazy podobné následujícímu příkladu:

```
DEFINE CHANNEL(TO.QMB) CHLTYPE(SDR) TRPTYPE(TCP) CONNAME(QMB.MACH.COM) XMITQ(QMB)
SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA256) DESCR('Sender channel using TLS from QMA to QMB')

DEFINE QLOCAL(QMB) USAGE(XMITQ)
```

Výsledky

Kanál odesilatele, TO.QMBa přenosová fronta QMB.

z/OS *Definování přijímacího kanálu v QMB na z/OS*

Pomocí příkazu **DEFINE CHANNEL** nastavte požadovaný objekt.

Postup

V systému QMB zadejte příkaz podobný následujícímu příkladu:

```
DEFINE CHANNEL(TO.QMB) CHLTYPE(RCVR) TRPTYPE(TCP) SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA256)
SSLCAUTH(REQUIRED) DESCR('Receiver channel using TLS to QMB')
```

Výsledky

Přijímací kanál TO.QMB, je vytvořen.

z/OS *Spuštění kanálu odesilatele v systému QMA v systému z/OS*

V případě potřeby spusťte program listener a obnovte zabezpečení. Poté spusťte kanál pomocí příkazu **START CHANNEL** .

Postup

1. Volitelné: Pokud jste tak dosud neučinili, spusťte program listener na QMB.

   Program listener naslouchá příchozím síťovým požadavkům a spustí přijímací kanál v případě potřeby. Informace o tom, jak spustit modul listener, naleznete v tématu Spuštění modulu listener kanálu.
2. Volitelné: Pokud byly některé kanály SSL/TLS spuštěny dříve, zadejte příkaz `REFRESH SECURITY TYPE(SSL)`.

   Tím zajistíte, že všechny změny provedené v úložišti klíčů budou k dispozici.
3. Spusťte kanál na QMA pomocí příkazu `START CHANNEL(TO.QMB)`.

Výsledky

Kanál odesilatele je spuštěn.

z/OS *Výměna certifikátů podepsaných svým držitelem na systému z/OS*

Vyměňte certifikáty, které jste předtím extrahovali. Pokud používáte FTP, použijte správný formát.

Postup

Přeneste část CA certifikátu QM1 do systému QM2 a naopak, například pomocí FTP.

Pokud přenášíte certifikáty pomocí protokolu FTP, musíte tak učinit ve správném formátu.

Přeneste následující typy certifikátů v *binárním* formátu:

- Binární soubor kódovaný DER X.509
- PKCS #7 (certifikáty CA)

- PKCS #12 (osobní certifikáty)

Přeneste následující typy certifikátů ve formátu ASCII:

- PEM (ochrana osobních údajů-rozšířená pošta)
- Base64 kódovaný X.509

z/OS *Definování kanálu odesilatele a přenosové fronty v systému QM1 v systému z/OS*

Pomocí příkazů **DEFINE CHANNEL** a **DEFINE QLOCAL** nastavte požadované objekty.

Postup

V systému QM1zadejte příkazy podobné následujícímu příkladu:

```
DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(SDR) TRPTYPE(TCP) CONNAME(QM1.MACH.COM) XMITQ(QM2)
SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA) DESCR('Sender channel using TLS from QM1 to QM2')

DEFINE QLOCAL(QM2) USAGE(XMITQ)
```

CipherSpecs na obou koncích kanálu musí být stejné.

Chcete-li, aby kanál používal protokol TLS, je povinný pouze parametr SSLCIPH. Informace o povolených hodnotách parametru SSLCIPH naleznete v části “CipherSpecs a CipherSuites v souboru IBM MQ” na stránce 41 .

Výsledky

Kanál odesilatele QM1.TO.QM2a přenosová fronta QM2.

z/OS *Definování přijímacího kanálu na QM2 na z/OS*

Pomocí příkazu **DEFINE CHANNEL** nastavte požadovaný objekt.

Postup

V systému QM2zadejte příkaz podobný následujícímu příkladu:

```
DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(RCVR) TRPTYPE(TCP) SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA256)
SSLCAUTH(REQUIRED) DESCR('Receiver channel using TLS from QM1 to QM2')
```

Kanál musí mít stejný název jako kanál odesilatele, který jste definovali v souboru “Definování kanálu odesilatele a přenosové fronty v systému QM1 v systému z/OS” na stránce 341, a musí používat stejnou CipherSpec.

z/OS *Spuštění kanálu odesilatele v systému QM1 v systému z/OS*

V případě potřeby spusťte program listener a obnovte zabezpečení. Poté spusťte kanál pomocí příkazu **START CHANNEL** .

Postup

1. Volitelné: Pokud jste tak dosud neučinili, spusťte program listener na serveru QM2.

   Program listener naslouchá příchozím síťovým požadavkům a spustí přijímací kanál v případě potřeby. Informace o spuštění modulu listener naleznete v tématu Spuštění modulu listener kanálu .
2. Volitelné: Pokud byly některé kanály SSL/TLS spuštěny dříve, zadejte příkaz REFRESH SECURITY TYPE (SSL).

   Tím zajistíte, že všechny změny provedené v úložišti klíčů budou k dispozici.
3. V systému QM1spusťte kanál pomocí příkazu `START CHANNEL(QM1.TO.QM2)`.

Výsledky

Kanál odesilatele je spuštěn.

z/OS *Aktualizace prostředí SSL nebo TLS v systému z/OS*

Aktualizujte prostředí TLS ve správci front QMA pomocí příkazu **REFRESH SECURITY** .

Postup

V systému QMA zadejte následující příkaz:

```
REFRESH SECURITY TYPE(SSL)
```

Tím zajistíte, že všechny změny provedené v úložišti klíčů budou k dispozici.

z/OS *Povolení anonymních připojení v přijímacím kanálu v systému z/OS*

Pomocí příkazu **ALTER CHANNEL** můžete nastavit ověřování klienta SSL nebo TLS jako volitelné.

Postup

V systému QMB zadejte následující příkaz:

```
ALTER CHANNEL(TO.QMB) CHLTYPE(RCVR) SSLCAUTH(OPTIONAL)
```

z/OS *Spuštění kanálu odesilatele v systému QM1 v systému z/OS*

V případě potřeby spusťte inicializátor kanálu, spusťte program modulu listener a obnovte zabezpečení. Poté spusťte kanál pomocí příkazu **START CHANNEL** .

Postup

1. Volitelné: Pokud jste tak dosud neučinili, spusťte inicializátor kanálu.
2. Volitelné: Pokud jste tak dosud neučinili, spusťte program listener na serveru QM2.

   Program listener naslouchá příchozím síťovým požadavkům a spustí přijímací kanál v případě potřeby. Informace o spuštění modulu listener naleznete v tématu Spuštění modulu listener kanálu .
3. Volitelné: Pokud byl inicializátor kanálu již spuštěn nebo byly dříve spuštěny kanály SSL/TLS, zadejte příkaz REFRESH SECURITY TYPE (SSL).

   Tím zajistíte, že všechny změny provedené v úložišti klíčů budou k dispozici.
4. V systému QM1spusťte kanál pomocí příkazu `START CHANNEL(QM1.TO.QM2)`.

Výsledky

Kanál odesilatele je spuštěn.

z/OS *Spuštění kanálu odesilatele v systému QMA v systému z/OS*

V případě potřeby spusťte inicializátor kanálu, spusťte program modulu listener a obnovte zabezpečení. Poté spusťte kanál pomocí příkazu **START CHANNEL** .

Postup

1. Volitelné: Pokud jste tak dosud neučinili, spusťte inicializátor kanálu.
2. Volitelné: Pokud jste tak dosud neučinili, spusťte program listener na QMB.

   Program listener naslouchá příchozím síťovým požadavkům a spustí přijímací kanál v případě potřeby. Informace o tom, jak spustit modul listener, naleznete v tématu Spuštění modulu listener kanálu.
3. Volitelné: Pokud byl inicializátor kanálu již spuštěn nebo pokud byly dříve spuštěny kanály SSL/TLS, zadejte příkaz `REFRESH SECURITY TYPE(SSL)`.

Tím zajistíte, že všechny změny provedené v úložišti klíčů budou k dispozici.

4. Spusťte kanál na QMA pomocí příkazu START CHANNEL(TO.QMB).

Výsledky

Kanál odesilatele je spuštěn.

z/OS *Úprava délky klíče eliptické křivky na z/OS*

Jak upravit proměnnou prostředí GSK_CLIENT_ECURVE_LIST, abyste nastavili seznam eliptických křivek nebo podporovaných skupin, které jsou určeny klientem, jako řetězec skládající se z jedné nebo více 4znakových hodnot v pořadí podle předvolby pro použití.

Důležité: Musíte použít opravu v z/OS APAR OA61783 , chcete-li povolit, aby operační systém použil určité eliptické křivky při použití TLS 1.0, TLS 1.1 a/nebo TLS 1.2 vyjednaných připojení.

Tuto proměnnou prostředí TLS můžete nastavit ve spouštěcím JCL inicializátoru kanálu pomocí příkazu CEEOPTS DD:

```
CEEOPTS DD DSN=<dataset-name>,DISP=SHR
```

Ve výše uvedené datové sadě zadejte seznam, který chcete použít, například:

```
ENVAR("GSK_CLIENT_ECURVE_LIST=002300240025")
```

Důležité: Nepoužívejte tento příkaz CEEOPTS s daty in-stream, protože to brání nastavení proměnné prostředí pro všechny úlohy TLS používající tento příkaz.

Ujistěte se, že odkazujete na sekvenční datovou sadu nebo člena dělené datové sady, abyste umožnili tuto práci při použití hodnoty SSLTASKS větší než jedna.

Můžete také použít analogový ekvivalent serveru GSK_CLIENT_ECURVE_LIST, což je GSK_SERVER_ALLOWED_KEX_ECURVES. Další informace viz Omezení eliptických křivek výměny klíčů .

Kromě toho viz tabulka 5 v Definicích čipových sad , kde je uveden seznam platných 4znakových eliptických křivek a podporovaných specifikací skupin.

Výchozí specifikace je 00210023002400250019. Je-li povoleno zabezpečení TLS V1.3 , 0029 (x25519) se připojí na konec výchozího seznamu.

Identifikace a ověřování uživatelů

Uživatele můžete identifikovat a ověřit pomocí certifikátů X.509 , struktury MQCSP nebo několika typů uživatelského programu.

Použití certifikátů X.509

Uživatele můžete identifikovat a ověřit pomocí certifikátů X.509 s příkazem **SET CHLAUTH** a parametrem **SSLPEER** . Parametr **SSLPEER** určuje filtr, který má být použit pro porovnání s rozlišujícím názvem předmětu certifikátu od správce front typu peer nebo klienta na druhém konci kanálu.

Další informace o použití příkazu **SET CHLAUTH** a parametru **SSLPEER** viz SET CHLAUTH.

Digitální certifikáty mohou být odvolány certifikačním úřadem. V závislosti na platformě můžete zkontrolovat stav odvolání certifikátů pomocí protokolu OCSP nebo seznamů CRL na serverech LDAP. Další informace viz téma “Práce se zrušenými certifikáty” na stránce 359.

Použití struktury MQCSP

Struktura parametrů zabezpečení připojení MQCSP je určena ve volání MQCONNX. Tato struktura může obsahovat pověření dodaná aplikací. Aplikace může zadat ID uživatele a heslo ve struktuře MQCSP.

Od IBM MQ 9.3.4mohou aplikace také dodat token ověření. V případě potřeby lze MQCSP změnit v uživatelské proceduře zabezpečení.

Varování: Pověření ve struktuře MQCSP jsou někdy odesílána po síti jako prostý text. Chcete-li se ujistit, že jsou pověření aplikace klienta chráněna, prohlédněte si téma “Ochrana heslem MQCSP” na stránce 31.

Další informace naleznete v tématech “Identifikace a ověřování uživatelů pomocí struktury MQCSP” na stránce 345 a “Práce s tokeny ověření” na stránce 349.

Linux AIX V systémech AIX a Linuxlze ID uživatele a heslo určené ve struktuře MQCSP ověřit buď pomocí operačního systému, nebo pomocí metody PAM (Pluggable Authentication Method). Modul PAM poskytuje obecný mechanizmus pro ověřování uživatelů, který skrývá podrobnosti ze služeb. Další informace viz téma “Použití metody PAM (Pluggable Authentication Method)” na stránce 370.

Implementace identifikace a ověření v uživatelských procedur

Uživatele můžete identifikovat a ověřit pomocí několika typů uživatelského programu. Další informace naleznete v tématu “Implementace identifikace a ověřování v uživatelských procedur zabezpečení” na stránce 346, “Mapování identit v uživatelských procedur zpráv” na stránce 347 a “Mapování identit v uživatelské proceduře rozhraní API a uživatelské proceduře pro přechod rozhraní API” na stránce 348.

Oprávnění uživatelé

Privilegovaný uživatel je ten, který má úplná administrativní oprávnění pro IBM MQ.

Kromě uživatelů uvedených v následující tabulce existují určité objekty a autorizace, u nichž je třeba při udělování přístupu věnovat zvláštní pozornost, aby byla zajištěna integrita a zabezpečení správce front. Zvláštní kontrola musí být uplatněna při udělování některého z těchto povolení:

- Jakákoli oprávnění k objektům SYSTEM
- Administrativní autorizace pro vytváření, změny a odstraňování objektů.

  z/OS V systému z/OSje toto oprávnění zabezpečením příkazů a oprávněním zabezpečení prostředků příkazů pro zadávání příkazů DEFINE, ALTER a DELETE.

  Multi Na všech ostatních platformách se jedná o autorizace administrace, například `+crt`, `+chg` a `+dlt`.
- Autorizace administrace pro vymazání front.

  z/OS V systému z/OSse jedná o oprávnění zabezpečení příkazů a oprávnění zabezpečení prostředků příkazů pro zadávání příkazů CLEAR.

  Multi Na všech ostatních platformách je toto oprávnění `+clr`.
- Administrativní autorizace pro zastavení kanálů, vrácení zpět nebo potvrzení zpráv.

  z/OS V systému z/OSje tato autorizace oprávnění zabezpečení příkazů a oprávnění zabezpečení prostředků příkazů k zadávání příkazů, jako jsou RESET CHANNEL, START CHANNEL a STOP CHANNEL.

  Multi Na všech ostatních platformách jsou tato oprávnění `+ctrl` a `+ctrlx`.
- Autorizace rozhraní MQI alternativního uživatele, která umožňuje aplikacím eskalovat oprávnění pro kontroly autorizace.

  z/OS V systému z/OSje toto oprávnění jakékoli oprávnění udělené alternativním profilům zabezpečení uživatele.

  Multi Na všech ostatních platformách je toto oprávnění `+altusr`.
- Kontextové autorizace, které aplikacím umožňují měnit kontext zabezpečení zpráv.

z/OS V systému z/OSje touto autorizací jakékoli oprávnění udělené kontextovým profilům zabezpečení.

Multi Na všech ostatních platformách jsou tato oprávnění `+setall` a `+setid`.

Jako obecný činitel by měly být aplikacím systému zpráv udělena pouze základní oprávnění MQI pro potřebné fronty nebo témata. Kanály MCA spouštěné pod neprivilegovaným uživatelem MCAUSER a některými dalšími speciálními typy aplikací, jako jsou obslužné rutiny fronty nedoručených zpráv, mohou vyžadovat další oprávnění, která nejsou běžně udělována aplikacím, aby fungovaly správně.

Tabulka 67. Oprávnění uživatelé podle platformy

Platforma	**Oprávnění uživatelé**
Systémy Windows	• SYSTÉM • Členové skupiny mqm • Členové skupiny Administrators
Systémy AIX and Linux	• Členové skupiny mqm
IBM i IBM i Systémy IBM i	• Profily qmqm a qmqmadm • Všichni členové skupiny qmqmadm • Jakýkoli uživatel definovaný s nastavením *ALLOBJ
z/OS	ID uživatele, pod kterým je spuštěn iniciátor kanálu, správce front a adresní prostory rozšířeného zabezpečení zpráv. Tato ID uživatelů nemají automaticky úplná administrativní oprávnění pro produkt IBM MQ, ale jsou považována za privilegovaná kvůli úrovni přístupu, která je obvykle udělována těmto ID uživatelů.

Identifikace a ověřování uživatelů pomocí struktury MQCSP

Můžete určit strukturu parametrů zabezpečení připojení MQCSP ve volání MQCONNX. Struktura MQCSP je primární způsob pro aplikace, které používají rozhraní fronty zpráv (MQI) k řízení pověření používaných pro ověřování.

Struktura MQCSP obsahuje pověření, které může autorizační služba použít k identifikaci a ověření uživatele.

Strukturu MQCSP lze upravit pomocí uživatelských procedur zabezpečení na straně klienta nebo serveru, a to i v případě, že aplikace strukturu MQCSP explicitně neposkytuje. Příkladem aplikace, která explicitně neposkytuje strukturu MQCSP, je aplikace, která používá produkt IBM MQ classes for JMS. Příklad uživatelské procedury zabezpečení na straně klienta, která vkládá ID uživatele a heslo do struktury MQCSP, viz “Uživatelská procedura zabezpečení na straně klienta pro vložení ID uživatele a hesla (mqccred)” na stránce 79.

V 9.3.4 Struktura MQCSP obsahuje ID uživatele a heslo nebo token ověření. Pro pověření dodaná ve struktuře MQCSP platí následující omezení:

- Aplikace nebo uživatelská procedura musí zadat buď ID uživatele a heslo, nebo token ověření, ale ne obojí.
- Pro přístup k produktu IBM MQlze použít pouze tokeny ověření, které splňují specifické formáty a požadavky. Další informace o požadavcích na tokeny ověření v IBM MQviz “Požadavky na tokeny ověření” na stránce 351.

- Má-li být identita v tokenu ověření převzata jako kontext pro aplikaci, musí token poskytnout vhodný nárok uživatele a hodnota nároku musí být platné ID uživatele IBM MQ . Například jméno uživatele musí splňovat omezení maximální délky a speciálních znaků. Další informace o převzetí ID uživatele viz “Relace mezi MQCSP a nastavením CTX po připojení” na stránce 346.

Další informace o struktuře MQCSP viz Parametry zabezpečení MQCSP.

Varování: Pověření ve struktuře MQCSP pro klientskou aplikaci jsou někdy odesílána po síti jako prostý text. Chcete-li se ujistit, že jsou pověření aplikace klienta chráněna, prohlédněte si téma “Ochrana heslem MQCSP” na stránce 31.

Relace mezi MQCSP a nastavením CTX po připojení

Produkt IBM MQ vždy ověřuje pověření předaná ve struktuře MQCSP, je-li povolena funkce ověřování připojení. Po úspěšném ověření pověření může produkt IBM MQ převzít ID uživatele pro následné kontroly autorizace operací provedených připojenou aplikací. ID uživatele v pověřeních MQCSP je převzata, pokud je objekt ověřovacích informací (AUTHINFO), na který odkazuje atribut **CONNAUTH** správce front, definován s hodnotou **ADOPTCTX(YES)**.

IBM MQ má limit délky ID uživatelů, které může použít pro kontroly autorizace. Další informace o těchto limitech viz “ID uživatelů” na stránce 88. Při přijetí ID uživatele předaného ve struktuře MQCSP se produkt IBM MQ chová odlišně v závislosti na dalších volbách konfigurace:

- Při použití ověření připojení LDAP produkt IBM MQ převezme ID uživatele, které je v atributu krátkého jména uživatele záznamu LDAP uživatele. Atribut krátkého jména uživatele se nastavuje pomocí atributu **SHORTUSR** objektu AUTHINFO.

  Pokud je například parametr **SHORTUSR** nastaven na hodnotu `'CN'` a záznam LDAP uvádí uživatele jako `'CN=Test,SN=MQ,O=IBM,C=UK'`, použije se ID uživatele `Test` .
- Používáte-li ověření připojení operačního systému nebo ověření PAM, je-li hodnota pole ADOPTCTX YES, je ID uživatele předané ve struktuře MQCSP zkráceno, aby splňovalo 12znakový limit ID uživatele IBM MQ , když je převzat jako kontext připojení.

  Je-li povolena volba **ChlAuthEarlyAdopt** , dojde k oříznutí po ověření pověření uživatele.

  Není-li volba **ChlAuthEarlyAdopt** povolena, dojde k oříznutí před přijetím. Pokud je v systému Windowsuživatel dodán ve formátu `user@domain`, znamená to, že oříznutí může vést ke specifikaci domény, která není platná, pokud je uživatel kratší než 12 znaků.

  Pokud je například uživatel `` `ibmmq@windowsdomain` `` poskytnut prostřednictvím MQCSP, je v tomto scénáři zkrácen na `` `ibmmq@window` `` . To má za následek následující chybu:

  ```
  AMQ8074W: Autorizace se nezdařila, protože SID 'SID' neodpovídá entitě 'ibmmq@window'
  ```

  Na tomto základě, pokud předáte ID uživatele delší než 12 znaků, jako např. ID uživatele domény Windows ve tvaru `user@domain`, prostřednictvím MQCSP byste měli nakonfigurovat **ChlAuthEarlyAdopt**=*Y* v souboru qm.ini , abyste se vyhnuli této chybě.

  Alternativně použijte volbu ADOPTCTX (NO) v konfiguraci CONNAUTH AUTHINFO a použijte alternativní přístup, jako např. pravidlo CHLAUTH USERMAP, uživatelskou proceduru zabezpečení nebo nastavení objektu kanálu MCAUSER, abyste nastavili ID uživatele pro kanál.

Implementace identifikace a ověřování v uživatelských procedur zabezpečení

Uživatelskou proceduru zabezpečení můžete použít k implementaci jednosměrného nebo vzájemného ověření.

Primárním účelem uživatelské procedury zabezpečení je umožnit MCA na každém konci kanálu ověřit svého partnera. Na každém konci kanálu zpráv a na konci serveru kanálu MQI agent MCA obvykle jedná jménem správce front, ke kterému je připojen. Na straně klienta kanálu MQI agent MCA obvykle jedná jménem uživatele aplikace IBM MQ MQI client . V této situaci probíhá vzájemné ověřování mezi dvěma správci front nebo mezi správcem front a uživatelem aplikace IBM MQ MQI client .

Zadaná uživatelská procedura zabezpečení (uživatelská procedura kanálu SSPI) ilustruje, jak lze vzájemné ověřování implementovat prostřednictvím výměny tokenů ověřování, které jsou generovány a poté kontrolovány důvěryhodným ověřovacím serverem, například Kerberos. Další informace naleznete v tématu “Uživatelský program kanálu SSPI v systému Windows” na stránce 155.

Vzájemné ověřování lze také implementovat pomocí technologie PKI (Public Key Infrastructure). Každá uživatelská procedura zabezpečení vygeneruje náhodná data, podepíše je pomocí soukromého klíče správce front nebo uživatele, kterého zastupuje, a odešle podepsaná data svému partnerovi ve zprávě zabezpečení. Uživatelská procedura zabezpečení partnera provede ověření kontrolou digitálního podpisu pomocí veřejného klíče správce front nebo uživatele. Před výměnou digitálních podpisů může být nutné, aby uživatelské procedury zabezpečení souhlasily s algoritmem pro generování kódu digest zprávy, pokud je k dispozici více než jeden algoritmus.

Když uživatelská procedura zabezpečení odešle podepsaná data svému partnerovi, musí také odeslat některé prostředky k identifikaci správce front nebo uživatele, kterého zastupuje. Může se jednat o rozlišující název nebo dokonce digitální certifikát. Je-li odeslán digitální certifikát, může partnerská uživatelská procedura zabezpečení certifikát ověřit tak, že bude pracovat v řetězu certifikátů s kořenovým certifikátem CA. To poskytuje záruku vlastnictví veřejného klíče, který se používá ke kontrole digitálního podpisu.

Uživatelská procedura zabezpečení partnera může ověřit digitální certifikát pouze v případě, že má přístup k úložišti klíčů, které obsahuje zbývající certifikáty v řetězu certifikátů. Není-li digitální certifikát pro správce front nebo uživatele odeslán, musí být k dispozici v úložišti klíčů, ke kterému má partnerská uživatelská procedura zabezpečení přístup. Uživatelská procedura zabezpečení partnera nemůže zkontrolovat digitální podpis, pokud nenajde veřejný klíč podepisujícího subjektu.

TLS (Transport Layer Security) používá právě popsané techniky PKI. Další informace o tom, jak SSL (Secure Sockets Layer) provádí ověření, viz “Koncepce TLS (Transport Layer Security)” na stránce 18.

Pokud není k dispozici důvěryhodný ověřovací server nebo podpora PKI, lze použít jiné techniky. Běžná technika, kterou lze implementovat v uživatelských procedur zabezpečení, používá algoritmus symetrického klíče.

Jedna z uživatelských procedur zabezpečení, exit A, vygeneruje náhodné číslo a odešle je ve zprávě zabezpečení do své partnerské uživatelské procedury zabezpečení, exit B. Ukončení B zašifruje číslo pomocí kopie klíče, která je známa pouze dvěma uživatelským procedurám zabezpečení. Ukončení B odešle zašifrované číslo pro ukončení A ve zprávě zabezpečení s druhým náhodným číslem, které bylo vygenerováno při ukončení B. Exit A ověří, že první náhodné číslo bylo správně zašifrováno, zašifruje druhé náhodné číslo pomocí jeho kopie klíče a odešle zašifrované číslo pro ukončení B ve zprávě zabezpečení. Ukončení B pak ověří, že druhé náhodné číslo bylo správně zašifrováno. Pokud během této výměny není uživatelská procedura zabezpečení spokojena s autenticitou jiné, může instruovat agenta MCA, aby kanál uzavřel.

Výhodou této techniky je, že během výměny není přes komunikační připojení odeslán žádný klíč nebo heslo. Nevýhodou je, že neposkytuje řešení problému, jak distribuovat sdílený klíč bezpečným způsobem. Jedno řešení tohoto problému je popsáno v tématu “Implementace důvěrnosti v uživatelských programech” na stránce 485. Podobná technika se používá v SNA pro vzájemné ověření dvou jednotek LU, když se vážou k vytvoření relace. Tato technika je popsána v části “Ověření na úrovni relace” na stránce 121.

Všechny předchozí techniky vzájemné autentizace lze přizpůsobit tak, aby poskytovaly jednosměrnou autentizaci.

Mapování identit v uživatelských procedur zpráv

Uživatelské procedury zpráv můžete použít ke zpracování informací pro ověření ID uživatele, i když může být lepší implementovat ověření na úrovni aplikace.

Když aplikace vloží zprávu do fronty, pole *UserIdentifier* v deskriptoru zprávy obsahuje ID uživatele přidružené k aplikaci. Nejsou však k dispozici žádná data, která by bylo možné použít k ověření ID uživatele. Tato data mohou být přidána uživatelskou procedurou pro zprávy na odesílajícím konci kanálu

a kontrolována uživatelskou procedurou pro zprávy na přijímacím konci kanálu. Data ověřování mohou být například šifrované heslo nebo digitální podpis.

Tato služba může být efektivnější, pokud je implementována na úrovni aplikace. Základním požadavkem je, aby uživatel aplikace, který obdrží zprávu, mohl identifikovat a ověřit uživatele aplikace, která odeslala zprávu. Je proto přirozené uvažovat o zavedení této služby na úrovni aplikace. Další informace viz "Mapování identit v uživatelské proceduře rozhraní API a uživatelské proceduře pro přechod rozhraní API" na stránce 348.

Mapování identit v uživatelské proceduře rozhraní API a uživatelské proceduře pro přechod rozhraní API

Aplikace, která přijme zprávu, musí být schopna identifikovat a ověřit uživatele aplikace, která zprávu odeslala. Tato služba je obvykle nejlépe implementována na úrovni aplikace. Uživatelské procedury rozhraní API mohou službu implementovat mnoha způsoby.

Na úrovni jednotlivých zpráv je identifikace a ověření službou, která zahrnuje dva uživatele, odesilatele a příjemce zprávy. Základním požadavkem je, aby uživatel aplikace, který obdrží zprávu, mohl identifikovat a ověřit uživatele aplikace, která odeslala zprávu. Všimněte si, že požadavek je jednosměrný, ne dvousměrný, ověření.

V závislosti na tom, jak je implementován, mohou uživatelé a jejich aplikace potřebovat rozhraní nebo dokonce interakci se službou. Kromě toho, kdy a jak se služba používá, může záviset na tom, kde jsou uživatelé a jejich aplikace umístěny, a na povaze samotných aplikací. Je proto přirozené uvažovat o zavedení služby na úrovni aplikace, a nikoli na úrovni propojení.

Pokud uvažujete o implementaci této služby na úrovni odkazu, možná budete muset vyřešit následující problémy:

- Jak na kanálu zpráv použijete službu pouze na ty zprávy, které ji vyžadují?
- Jak povolíte uživatelům a jejich aplikacím rozhraní nebo interakci se službou, pokud je to požadavek?
- V situaci s více přechody, kdy je zpráva odeslána přes více než jeden kanál zpráv na cestě do místa určení, kde vyvoláte komponenty služby?

Zde je několik příkladů, jak lze službu identifikace a ověření implementovat na úrovni aplikace. Termín *uživatelská procedura rozhraní API* znamená buď uživatelskou proceduru rozhraní API, nebo přechodovou uživatelskou proceduru rozhraní API.

- Když aplikace vloží zprávu do fronty, uživatelská procedura rozhraní API může získat token ověření od důvěryhodného ověřovacího serveru, například Kerberos. Uživatelská procedura rozhraní API může přidat tento token do dat aplikace ve zprávě. Je-li zpráva načtena přijímající aplikací, může druhá uživatelská procedura rozhraní API požádat ověřovací server o ověření odesilatele kontrolou tokenu.
- Když aplikace vloží zprávu do fronty, uživatelská procedura rozhraní API může k datům aplikace ve zprávě připojit následující položky:
  - Digitální certifikát odesílatele
  - Digitální podpis odesílatele

  Jsou-li pro použití k dispozici různé algoritmy pro generování kódu digest zprávy, může uživatelská procedura rozhraní API obsahovat název algoritmu, který použila.

  Když přijímající aplikace načte zprávu, druhá uživatelská procedura rozhraní API může provést následující kontroly:

  - Uživatelská procedura rozhraní API může ověřit digitální certifikát tak, že bude pracovat prostřednictvím řetězu certifikátů s kořenovým certifikátem CA. Chcete-li to provést, uživatelská procedura rozhraní API musí mít přístup k úložišti klíčů, které obsahuje zbývající certifikáty v řetězu certifikátů. Tato kontrola zajišťuje, že odesílatel identifikovaný rozlišujícím názvem je skutečným vlastníkem veřejného klíče obsaženého v certifikátu.
  - Uživatelská procedura rozhraní API může zkontrolovat digitální podpis pomocí veřejného klíče obsaženého v certifikátu. Tato kontrola ověřuje odesilatele.

Namísto celého digitálního certifikátu lze odeslat rozlišující název odesílatele. V tomto případě musí úložiště klíčů obsahovat certifikát odesílatele, aby druhá uživatelská procedura rozhraní API mohla najít veřejný klíč odesílatele. Další možností je odeslat všechny certifikáty v řetězu certifikátů.

- Když aplikace vloží zprávu do fronty, pole *UserIdentifier* v deskriptoru zprávy obsahuje ID uživatele přidružené k aplikaci. ID uživatele lze použít k identifikaci odesílatele. Chcete-li povolit ověření, uživatelská procedura rozhraní API může připojit některá data, například šifrované heslo, k datům aplikace ve zprávě. Když je zpráva načtena přijímající aplikací, druhá uživatelská procedura rozhraní API může ověřit ID uživatele pomocí dat, která byla se zprávou prošla.

  Tuto techniku lze považovat za dostatečnou pro zprávy, které pocházejí z řízeného a důvěryhodného prostředí, a za okolností, kdy není k dispozici důvěryhodný ověřovací server nebo podpora PKI.

Linux V 9.3.4 AIX Práce s tokeny ověření

Z aplikací klienta IBM MQ 9.3.4 mohou poskytovat tokeny pro ověření se správcem front spuštěným v operačním systému AIX nebo Linux. ID uživatele v tokenu lze také použít pro autorizaci pro přístup k prostředkům IBM MQ .

JWT (Webové tokeny JSON) přebírají model identity založený na deklaracích. Identita a řízení přístupu jsou abstrahovány do myšlenek nároků a vydavatelů tokenů.

- Nárok je dvojice název-hodnota, která obsahuje informace o uživateli a určuje, kdo je uživatel, ne co může dělat.
- Vydavatel tokenu je důvěryhodná třetí strana nebo server, který vydává token pro uživatele pouze na základě identity uživatele. Vydavatel tokenu se nezajímá o to, co může uživatel dělat.

Token je jednoduchá struktura, která obsahuje nároky a může být snadno převeden mezi stranami přes internet. Použití tokenů pro ověření má výhodu centralizované správy identit. Můžete použít jednoho vydavatele důvěryhodného tokenu, aby se vaše aplikace mohly ověřit s mnoha službami bez samostatné registrace u každé služby. Tokeny poskytují zvýšené zabezpečení, protože pověření nejsou odesílána každé službě, pouze důvěryhodnému vydavateli.

Token JWT je definován prostřednictvím navrhovaného internetového standardu RFC7519.

Jak tokeny pracují s produktem IBM MQ

Tokeny používané s produktem IBM MQ musí být platnými tokeny JWT, které byly podepsány algoritmem podporovaným produktem IBM MQ . Token JWT musí být podepsán podle standardu JWS (JSON Web Signature). Tokeny, které používají technologie JWE (JSON Web Encryption) a JWK (JSON Web Key) JOSE, nelze použít s produktem IBM MQ. Další informace viz “Požadavky na tokeny ověření” na stránce 351.

Aplikace, která dodává token ověření, může být spuštěna na libovolné platformě, která podporuje produkt IBM MQ clients. Aplikace musí být napsána v jazyce C V 9.3.5 nebo, z adresáře IBM MQ 9.3.5, v adresáři Java a připojit se ke správci front pomocí vazeb klienta. Správce front však musí být spuštěn v operačním systému AIX nebo Linux. Správce front musí být konfigurován tak, aby přijímal tokeny ověřování. Úložiště klíčů musí obsahovat certifikát veřejného klíče nebo symetrický klíč vydavatele důvěryhodného tokenu, v závislosti na algoritmu použitém k podepsání tokenu.

Vydavatel tokenu je důvěryhodná strana, která má delegovaný přístup zabezpečení, což znamená, že ověřuje identitu uživatele aplikace. Správce front kontroluje, zda je token ověření platný a zda je ověřený uživatel autorizován pro přístup k objektům produktu IBM MQ . Správce front může, ale nemusí vědět o uživatelích dříve, než se poprvé připojí pomocí tokenu. Administrátor produktu IBM MQ musí nastavit ověření a autorizaci pro aplikace, které se připojují ke správci front, a nastavit požadavky na to, co musí tokeny obsahovat.

Aplikace klienta může dynamicky požadovat token od vydavatele, který používá pro ověření při připojení k produktu IBM MQ. Aplikace poté použije strukturu MQCSP V 9.3.5 nebo z produktu IBM MQ 9.3.5ekvivalent ve zvoleném rozhraní API k předání tokenu správci front při připojení.

Pokud aplikaci nelze změnit tak, aby požadovala token ověření, a prezentovat token správci front při připojení, lze uživatelskou proceduru zabezpečení alternativně použít k poskytnutí tokenu ve struktuře MQCSP.

Pokud token splňuje požadavky na tokeny ověření a podpis tokenu je platný, vytvoří se připojení. Správce front může také použít ID uživatele obsažené v tokenu pro kontroly autorizace pro přístup k prostředkům produktu IBM MQ , pokud je v tokenu obsažen volitelný nárok uživatele. Nárok uživatele je nárok v rámci tokenu, který obsahuje ID uživatele, které správce front přijímá pro kontroly autorizace. Tento název nároku uživatele je uveden s atributem **`UserClaim`** v sekci **`AuthToken`** souboru `qm.ini` .

Další informace viz “Použití tokenů ověření v aplikaci” na stránce 357 a Parametry zabezpečení MQCSP.

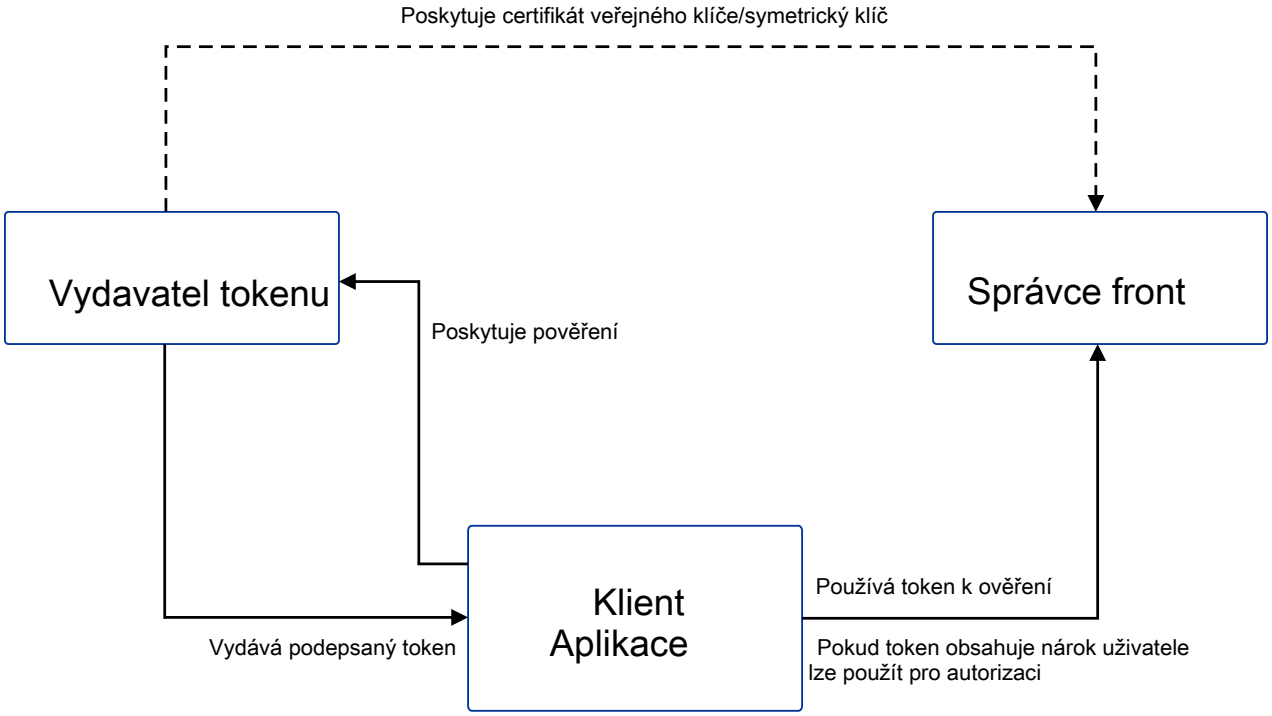


Diagram zobrazuje základní příklad očekávaného toku pro použití tokenů s IBM MQ. Očekávaný životní cyklus je následující:

- Token je vydán aplikaci důvěryhodným vydavatelem. Další informace viz Požadavky na tokeny ověření.
- Aplikace předá token správci front při připojení. Další informace naleznete v tématu Použití tokenů ověření v aplikaci.
- Správce front ověřuje podpis tokenu vůči důvěryhodnému veřejnému klíči vydavatele nebo symetrickému klíči v úložišti klíčů. Chcete-li nastavit správce front, postupujte podle pokynů v části Konfigurace správce front pro přijetí tokenů ověřování.
- Pokud token ověření obsahuje platný nárok uživatele, může být uživatel v tokenu převzat pro kontroly autorizace pro přístup k prostředkům IBM MQ . Další informace naleznete v tématu Přijetí uživatelů pro autorizaci.
- Administrátor produktu IBM MQ spravuje certifikáty vydavatele důvěryhodných tokenů. Po vypršení platnosti certifikátu je nutné získat nový certifikát od vydavatele tokenu a přidat jej do úložiště klíčů.
- Pokud jste nakonfigurovali svého správce front a aplikace se připojují, ale narazí na problémy s tokenem, přečtěte si téma Odstraňování problémů s tokeny ověření a Kódy chyb ověření tokenu.

Produkt IBM MQ pracuje s libovolným vydavatelem tokenů, který poskytuje tokeny odpovídající standardům JWT a JWS.

Pokud již tokeny nepoužíváte, ale chcete porozumět tomu, co se podílí na vytvoření serveru tokenů, prostudujte si příručku Začínáme pro bezplatný a otevřený projekt Keycloak.

Související odkazy

Sekce AuthToken souboru `qm.ini`

Linux V 9.3.4 AIX Požadavky na tokeny ověření

Požadavky na ověření, struktura a algoritmy pro tokeny ověření použité s produktem IBM MQ.

Požadavky

Tokeny ověření, které se používají s produktem IBM MQ , musí splňovat následující požadavky.

- Délka tokenu nesmí překročit maximální délku 8192 znaků. Další informace viz TokenLength (MQLONG) pro MQCSP.
- Struktura tokenu a kódování je platné, jak je definováno ve specifikaci JSON Web Token (JWT) v RFC7519a ve specifikaci JSON Web Signature (JWS) v RFC7515.
- Požadované parametry záhlaví tokenu, které jsou uvedeny v souboru Tabulka 68 na stránce 352 , jsou přítomny a hodnoty parametrů jsou platné.
- Požadované nároky na informační obsah uvedené v souboru Tabulka 69 na stránce 352 jsou přítomny a hodnoty nároků jsou platné.
- Token je podepsán algoritmem v adresáři Tabulka 70 na stránce 353 , který IBM MQ podporuje.
- Hodnota nároku vypršení platnosti (**exp**) je pozdější než aktuální čas.
- Pokud je přítomen nárok, který není před (**nbf**), hodnota je před aktuálním časem.
- Je-li uveden nárok uživatele, musí hodnota splňovat požadavky na “ID uživatelů v tokenech ověření” na stránce 353.

Struktura tokenu

Produkt IBM MQ přijímá JWT, které jsou v souladu se standardem RFC7519 . Token JWT musí být podepsán a zakódován podle standardu JWS, který je definován v RFC7515.

Produkt IBM MQ očekává, že zabezpečený token JWS bude obsahovat následující tři komponenty:

Záhlaví JOSE

Objekt JSON, který obsahuje parametry popisující typ tokenu a šifrovací algoritmy, které se používají k zabezpečení jeho obsahu.

Následující příklad záhlaví deklaruje, že kódovaný objekt je JWT a že záhlaví a informační obsah jsou zabezpečeny pomocí algoritmu HMAC SHA-256 .

```
{
 "typ":"JWT",
 "alg":"HS256"
}
```

Informační obsah JWS

Objekt JSON, který obsahuje nároky, jak je uvedeno ve standardu JWT. Každý člen objektu JSON je nárokem. Nároky mohou deklarovat identitu vydavatele tokenu nebo ID uživatele nositele.

```
{
 "exp": 1685529153,
 "nbf": 1685528150,
 "AppUser": "MyUserName"
 }
```

Podpis JWS

Používá se k ověření, že token je vydán důvěryhodným vydavatelem.

Tyto komponenty jsou v zabezpečeném tokenu JWS reprezentovány jako řetězce base64url-encoded oddělené tečkou ('.').

Token ověřování, který je v souladu se standardem JWS, je podepsán, aby bylo možné ověřit pravost tokenu, ale není šifrován. Proto jej může číst a případně znovu používat každý, kdo má přístup k tokenu. Konfigurujte připojení ke správci front, abyste se ujistili, že je ověření chráněno pomocí šifrování, když je odesláno přes síť, například pomocí TLS. Další informace o volbách ochrany pověření dodaných aplikací naleznete v tématu Ochrana pomocí hesla MQCSP.

Produkt IBM MQ podporuje následující parametry a nároky v záhlaví a informační obsah tokenů ověření. Všechny další parametry nebo nároky v tokenu jsou ignorovány. Pokud token obsahuje více než jeden parametr nebo nárok se stejným názvem, použije se poslední parametr nebo nárok s duplicitním názvem.

Tabulka 68. Popisy parametrů záhlaví tokenu

Část tokenu	Název parametru	Datový typ	Povinné	Popis
Header	**typ**	Řetězec	Ano	Typ tokenu. Hodnota tohoto parametru musí být "JWT".
	alg	Řetězec	Ano	Algoritmus použitý k zabezpečení záhlaví a informačního obsahu. Hodnota tohoto parametru musí být jedním z algoritmů v souboru Tabulka 70 na stránce 353.

Tabulka 69. Popisy nároků na informační obsah tokenu

Část tokenu	Název parametru	Datový typ	Povinné	Popis
Informační obsah	**exp**	Celé číslo	Ano	Čas vypršení platnosti tokenu, vyjádřený jako počet sekund od 1. ledna 1979, 00:00 koordinovaného univerzálního času. Token není po této době přijat.
	nbf	Celé číslo	Ne	Čas, vyjádřený jako počet sekund od 1. ledna 1979, 00:00 Koordinovaný univerzální čas, před kterým není token přijat.
	Název nároku uživatele uvedl v poli **UserClaim** sekce **AuthToken** v souboru `qm.ini` .	Řetězec	Vyžadováno pouze v případě, že je pro autorizaci použit nárok uživatele v tokenu.	Název nároku, který obsahuje ID uživatele adoptované pro kontroly autorizace. Pokud má například token nárok uživatele `"AppUser": "MyUserName"`, musíte zadat **UserClaim**=`AppUser` v sekci **AuthToken** souboru `qm.ini` .

Dobrý příklad kódovaného a dekódovaného tokenu naleznete na stránce ladicí program na webu `jwt.io` .

Algoritmy

Produkt IBM MQ podporuje podmnožinu algoritmů, které jsou obsaženy ve specifikaci JWA (JSON Web Algorithms) pro zabezpečené tokeny JWS .

Tabulka 70. Webové algoritmy JSON (JWA) podporované produktem IBM MQ pro zabezpečené tokeny JWS	
alg hodnota parametru	**Algoritmus digitálního podpisu nebo MAC**
HS256	HMAC používající SHA-256
HS384	HMAC používající SHA-384
HS512	HMAC používající SHA-512
RS256	RSASSA-PKCS1-v1_5 pomocí SHA-256
RS384	RSASSA-PKCS1-v1_5 pomocí SHA-384
RS512	RSASSA-PKCS1-v1_5 pomocí SHA-512

Požadavky na certifikát asymetrického klíče

Pokud je token podepsán asymetrickým klíčem, musí být certifikát veřejného klíče od vydavatele tokenu v úložišti klíčů, které správce front používá pro ověření tokenu. Když je token ověření přijat, musí být certifikát v období platnosti. Neprovádějí se žádné kontroly, aby se zajistilo, že certifikát od vydavatele tokenu nebyl odvolán.

ID uživatelů v tokenech ověření

Pokud je správce front nakonfigurován tak, aby převzal ID uživatele, které je obsaženo v nároku uživatele na token ověření, jako kontext pro aplikaci, musí ID uživatele, který je adoptován, splňovat následující požadavky:

- Může obsahovat až 12 znaků.
- Musí začínat jedním z následujících znaků:

  A-Z a-z
- Může obsahovat jakýkoli z následujících znaků:

  0-9 A-Z a-z +,-. : = _
- Nesmí se jednat o jedno z vyhrazených ID uživatelů UNKNOWN a NOBODY.

Související úlohy

Konfigurace správce front pro přijetí **AuthTokens**

Související odkazy

Sekce AuthToken souboru `qm.ini`

Linux V 9.3.4 AIX Konfigurace správce front pro přijetí tokenů ověřování

Nakonfigurujte svého správce front IBM MQ spuštěného v systému AIX nebo Linux , aby ověřoval uživatele a aplikace pomocí tokenů ověření.

Než začnete

Další informace o tom, jak tokeny pracují s produktem IBM MQ, Práce s tokeny ověření.

Před konfigurací správce front zkontrolujte, zda je objekt AUTHINFO, na který odkazuje atribut **CONNAUTH** správce front, typu `IDPWOS`. Ověřování tokenu je k dispozici pouze v případě, že je správce front konfigurován pro kontrolu ID uživatele a hesla operačního systému.

Zkontrolujte, že atribut **SecurityPolicy** sekce Service není nastaven na `Group`. Ověření tokenu není k dispozici, pokud je parametr **SecurityPolicy** explicitně nastaven na hodnotu `Skupina`. Je-li

parametr **SecurityPolicy** nastaven na hodnotu Skupina, odeberte atribut **SecurityPolicy** ze sekce služby a poté restartujte správce front.

Informace o této úloze

Z aplikací IBM MQ 9.3.4 se mohou ověřovat u správce front pomocí tokenů. Produkt IBM MQ přijímá webové tokeny JSON (*JWT*) od důvěryhodných vydavatelů, kteří dodržují navrhovaný internetový standard RFC7519. Tokeny můžete použít k ověření identity, která pak může být převzata pro budoucí kontroly autorizace.

Konfigurujte správce front tak, aby přijímal tokeny, a to uložením certifikátu veřejného klíče důvěryhodného vydavatele nebo symetrického klíče do úložiště klíčů správce front. Přidejte sekci AuthToken do souboru `qm.ini` a aktualizujte konfiguraci zabezpečení, aby správce front vyzvedl novou konfiguraci.

Postup

1. Vytvořte úložiště klíčů.
   a) Vytvořte úložiště klíčů pro certifikát veřejného klíče nebo symetrický klíč přijatý od důvěryhodného vydavatele. Můžete použít buď úložiště klíčů CMS s příponou souboru `.kdb` , nebo úložiště klíčů PKCS#12 s příponou souboru `.p12`.

   Zadáním následujícího příkazu vytvořte úložiště klíčů CMS :

   ```
   runmqakm -keydb -create -db /var/mqm/qmgrs/qm1/tokenissuer/key.kdb -pw MyKeystorePassword
   -type cms
   ```

   Pokud příkaz **runmqakm** vrátí chybu, viz kódy chyb runmqakm. Pokud je příkaz úspěšně dokončen, použijte příkaz `ls` k vypsání obsahu adresáře:

   ```
   ls -l /var/mqm/qmgrs/qm1/tokenissuer
   ```

   Zobrazí se následující soubory:

   ```
   -rw------- 1 adminuser mqm 88 Feb 22 07:50 key.crl
   -rw------- 1 adminuser mqm 88 Feb 22 07:50 key.kdb
   -rw------- 1 adminuser mqm 88 Feb 22 07:50 key.rdb
   ```

   b) V případě potřeby změňte vlastnictví skupiny pro soubory úložiště klíčů, které jste vytvořili, aby skupina mqm mohla mít přístup pro čtení. Na počátku má přístup k vytvořeným souborům pouze uživatel s oprávněním administrátora, který příkaz spustil.

   ```
   chgrp mqm /var/mqm/qmgrs/qm1/tokenissuer/key.*
   ```

   c) Změňte režim souborů úložiště klíčů, abyste přidali oprávnění ke čtení pro skupinu mqm. Například následující příkaz přidá oprávnění ke čtení/zápisu pro vlastníka souboru a oprávnění jen pro čtení pro skupinu.

   ```
   chmod 640 /var/mqm/qmgrs/qm1/tokenissuer/key.*
   ```

2. Zašifrujte heslo úložiště klíčů pomocí příkazu **runqmcred** a uložte zašifrovaný řetězec do souboru.
   a) Vytvořte soubor, který bude obsahovat počáteční klíč používaný k šifrování hesla úložiště klíčů.

   Soubor musí obsahovat počáteční klíč jako jeden řádek textu. Maximální délka počátečního klíče je 256 bajtů. Pokud jste již nastavili počáteční klíč pro správce front pomocí atributu správce front **INITKEY** , zkopírujte hodnotu atributu **INITKEY** do nového souboru. Pokud jste dosud nenastavili počáteční klíč pro správce front, vytvořte nový jedinečný šifrovací klíč a přidejte jej do počátečního souboru s klíči.

   Poznámka: Další informace viz INITKEY. Pokud počáteční klíč neuvedete, použije se výchozí. Je bezpečnější používat vlastní počáteční klíč.

Poznámka: Udělte minimální nezbytná oprávnění k počátečnímu souboru s klíči, aby byl obsah souboru zabezpečený. Počáteční soubor s klíči se používá pouze k šifrování hesla úložiště klíčů. Proto pouze administrátoři, kteří používají počáteční klíč k šifrování hesel, potřebují přístup ke čtení počátečního souboru s klíči.

b) Není-li počáteční klíč správce front již nastaven, nastavte hodnotu atributu **INITKEY** správce front na počáteční klíč, který jste vytvořili v kroku “2.a” na stránce 354. Pomocí příkazu **ALTER QMGR** nastavte počáteční klíč správce front. Příklad:

```
ALTER QMGR INITKEY('myEncrypt10nK3y')
```

c) Zadejte příkaz **runqmcred** k zašifrování hesla úložiště klíčů. Pomocí parametru **-sf** zadejte cestu k souboru, který obsahuje počáteční klíč.

```
runqmcred -sf initial.key
```

Po zobrazení výzvy zadejte heslo úložiště klíčů. Šifrované heslo je výstupem příkazu.

```
5724-H72 (C) Copyright IBM Corp. 1994, 2024.
Enter password:
**************
<QM>!2!b5rb01sMzFzc1ClZeQMryruWFM3HSm8DKyEaZK7qzWY=!TrWdU57DCDXM0Qah99I/Lg==
```

Zkopírujte řetězec na posledním řádku a uložte jej do souboru.

3. K přidání certifikátu veřejného klíče nebo symetrického klíče vydavatele tokenu do úložiště klíčů použijte jednu z následujících metod.

   - Chcete-li přidat certifikát veřejného klíče RSA do úložiště klíčů, zadejte následující příkaz:

     ```
     runmqakm -cert -add -db /var/mqm/qmgrs/qm1/tokenissuer/key.kdb -pw MyKeystorePassword
     -label keylabel
              -file keyfile
     ```

   - Chcete-li do úložiště klíčů přidat zakódovaný symetrický klíč base64 , zadejte následující příkaz:

     ```
     runmqakm -secretkey -add -db /var/mqm/qmgrs/qm1/tokenissuer/key.kdb -pw MyKeystorePassword
     -label keylabel
              -file keyfile -format ascii
     ```

   Kde *keylabel* je popisek, který se má připojit k certifikátu nebo tajnému klíči, a *keyfile* je název souboru, který obsahuje certifikát nebo zakódovaný tajný klíč base64 .

4. Přidejte sekci **AuthToken** a následující atributy do souboru `qm.ini` :

   - Cesta k úložišti klíčů určená pomocí atributu **KeyStore** .
   - Soubor, který obsahuje heslo pro úložiště klíčů určené pomocí atributu **KeyStorePwdFile** .
   - Popisek certifikátu nebo symetrického klíče, který jste přidali v kroku “3” na stránce 355, určený pomocí atributu **CertLabel** .

   Příklad:

   ```
   AuthToken:
      KeyStore=/var/mqm/qmgrs/qm1/tokenissuer/key.kdb
      KeyStorePwdFile=/var/mqm/qmgrs/qm1/tokenissuer/key.pw
      CertLabel=rsakey
   ```

   Kde `key.kdb` je název úložiště klíčů, které jste vytvořili v kroku “1.a” na stránce 354, a `key.pw` je soubor, který obsahuje šifrované heslo pro úložiště klíčů, které jste vytvořili v kroku “2.c” na stránce 355.

   Další informace o sekci **AuthToken** naleznete v sekci AuthToken souboru `qm.ini`.

5. Pokud je správce front nakonfigurován tak, aby převzal ID uživatele, které je obsaženo v nároku uživatele tokenu pro použití v následných kontrolách autorizace, přidejte atribut **UserClaim** do sekce **AuthToken** .

Chcete-li určit, zda je správce front konfigurován pro převzetí ID uživatele v tokenu, zadejte následující příkaz MQSC:

```
DISPLAY AUTHINFO(authinfo_name) ADOPTCTX
```

Kde *authinfo_name* je hodnota atributu **CONNAUTH** správce front. Pokud má atribut **ADOPTCTX** hodnotu YES, je správce front nakonfigurován tak, aby převzal ID uživatele v tokenu, a atribut **UserClaim** musí být uveden v sekci **AuthToken** .

Nastavte hodnotu atributu **UserClaim** na název nároku na token, který obsahuje ID uživatele, které má být adoptováno. Pokud například token obsahuje nárok `"AppUser": "MyUserName"`, přidejte do sekce **AuthToken** následující řádek:

```
UserClaim=AppUser
```

6. Aktualizujte konfiguraci zabezpečení správce front tak, aby konfigurace tokenů byla převzata ze souboru `qm.ini` . Spusťte příkaz **runmqsc** zadáním následujícího příkazu:

```
runmqsc qm1
```

pak zadejte následující příkaz MQSC:

```
REFRESH SECURITY TYPE(CONNAUTH)
```

Jak pokračovat dále

Spolupracujte s vývojáři, abyste jim pomohli pochopit, jak mohou používat tokeny v aplikacích k ověřování u správce front.

Související pojmy

Odstraňování problémů s tokeny ověření

Související úlohy

Použití tokenů ověření v aplikaci

Související odkazy

Sekce AuthToken souboru `qm.ini`

V 9.3.4 Získání tokenu ověření od vybraného vydavatele tokenu

Zapište aplikaci, abyste získali token ověření od vybraného vydavatele tokenu, když se připojí ke správci front IBM MQ .

Než začnete

Viz informace v části “Použití tokenů ověření v aplikaci” na stránce 357.

Procedura

- Způsob získání tokenu ověření a přesný obsah tokenu se liší mezi různými vydavateli tokenů.

  Zapište aplikaci pro interakci se zvoleným vydavatelem tokenu, abyste vyžádali a získali token ověření.

  Token ověření musí splňovat požadavky IBM MQ na tokeny ověření. Další informace o těchto požadavcích viz “Požadavky na tokeny ověření” na stránce 351.

  Pokud zamýšlíte převzít ID uživatele, které je obsaženo v nároku na token jako kontext pro aplikaci, musí token ověření také splňovat následující požadavky:

  – Token ověření musí obsahovat nárok, který odpovídá názvu nároku uživatele v konfiguraci ověřování tokenu správce front.

  – Hodnota nároku uživatele musí splňovat požadavky na ID uživatelů v tokenech ověření. Další informace viz téma “ID uživatelů v tokenech ověření” na stránce 353.

Výsledky

Nyní jste získali správně formátovaný JWT , který lze předložit produktu IBM MQ k ověření.

Související úlohy

Konfigurace správce front pro přijetí **AuthTokens**

Související odkazy

Sekce AuthToken souboru `qm.ini`

MQCSP-parametry zabezpečení

V 9.3.4 Použití tokenů ověření v aplikaci

Zapište aplikaci tak, aby poskytovala token ověření při připojení ke správci front IBM MQ .

Než začnete

V produktu IBM MQ 9.3.4mohou aplikace při připojení ke správci front dodat token ověření.

Žádost musí splňovat tyto požadavky:

- V 9.3.5 Musí být napsáno v jazyce C nebo Java (pomocí IBM MQ classes for JMS/ Jakarta Messaging)
- Musí se připojit ke správci front jako IBM MQ client. To znamená, že aplikace se musí připojit ke správci front prostřednictvím sítě namísto použití lokálních vazeb.
- Musí se připojit ke správci front, který je spuštěn v systému AIX nebo Linux.

Pokud aplikace tyto požadavky nesplňuje, připojení se nezdaří a aplikaci se vrátí kód příčiny MQRC_FUNCTION_NOT_SUPPORTED (2298).

Aplikace, která dodává token ověření, může být spuštěna na libovolné platformě, která podporuje produkt IBM MQ MQI clients.

Klienti, kteří používají automatické opětovné připojení klienta, nemohou při připojení dodat token ověření. Pokud aplikace dodá token ověření a určí volbu `MQCNO_RECONNECT` nebo `MQCNO_RECONNECT_Q_MGR` ve struktuře MQCNO, připojení se nezdaří a aplikaci se vrátí kód příčiny MQRC_RECONNECT_INCOMPATIBLE (2547). Další informace o automatickém opětovném připojení klienta naleznete v tématu Automatické opětovné připojení klienta.

Pokud kvůli těmto požadavkům nemůžete napsat aplikaci, aby dodala token ověření, můžete alternativně migrovat aplikaci tak, aby používala tokeny ověření pomocí uživatelské procedury zabezpečení klienta. Uživatelskou proceduru zabezpečení klienta lze zapsat pro nastavení tokenu ověření ve struktuře MQCSP. Další informace o uživatelských procedur zabezpečení naleznete v tématu uživatelské procedury zabezpečení pro připojení klienta.

V 9.3.5 V produktu IBM MQ 9.3.5mohou klientské aplikace systému JMS při připojování přímo poskytovat token (viz “Získání tokenu ověření od vybraného vydavatele tokenu” na stránce 356).
V systému IBM MQ 9.3.4mohou aplikace systému Java nepřímo poskytovat token prostřednictvím uživatelského programu. Další informace viz Třída Java MQCSP.

Informace o této úloze

Poznámka: Token ověřování, který je v souladu se standardem JWS (JSON Web Signature), je podepsán, aby bylo možné ověřit pravost tokenu, ale není šifrován. Proto jej může číst a případně znovu používat každý, kdo má přístup k tokenu. Konfigurujte připojení ke správci front, abyste se ujistili, že token ověření je chráněn pomocí šifrování, když je odeslán přes síť, například pomocí TLS. Další informace o volbách ochrany pověření dodaných aplikací viz “Ochrana heslem MQCSP” na stránce 31.

Před úpravou aplikací pro připojení pomocí tokenu zajistěte:

- Správce front byl konfigurován tak, aby přijímal tokeny ověřování, a to podle kroků uvedených v části “Konfigurace správce front pro přijetí tokenů ověřování” na stránce 353 .

- Vaše aplikace může získat platný token podle potřeby z vašeho ověřovacího serveru, viz "Získání tokenu ověření od vybraného vydavatele tokenu" na stránce 356.

Chcete-li dodat token ověření při připojení aplikace ke správci front IBM MQ , zahrňte následující proces.

Procedura

- Chcete-li dodat token ověření z aplikace C (MQI), postupujte takto:

  Aplikace se musí připojit pomocí MQCONNX (spíše než MQCONN) a dodat strukturu MQCSP :

  – Pole **AuthenticationType** musí být nastaveno na hodnotu MQCSP_AUTH_ID_TOKEN.
  – Verze struktury musí být nastavena na MQCSP_VERSION_3.
  – Pole **TokenPtr** nebo **TokenOffset** musí odkazovat na váš token ověření.
  – Pole **TokenLength** musí být nastaveno na délku tokenu ověření.

  Příklad kódu C pro připojení ke správci front pomocí MQCSP verze 3 a tokenu ověření:

```
MQCNO cno = {MQCNO_DEFAULT};   /* Connection options  */
MQCSP csp = {MQCSP_DEFAULT};   /* Security parameters */

char  token[MQ_CSP_TOKEN_LENGTH +1] = {0};  /* Authentication token string */

/* Set the connection options */
cno.SecurityParmsPtr = &csp;
cno.Version = MQCNO_VERSION_5;

/* Set the security parameters */
csp.Version = MQCSP_VERSION_3;
csp.AuthenticationType = MQCSP_AUTH_ID_TOKEN;
csp.TokenPtr = token;
csp.TokenLength = (MQLONG) strlen(token);

/* Connect to the queue manager */
MQCONNX(qmName,                 /* Queue manager name  */
        &cno,                   /* Connection options  */
        &hCon,                  /* Connection handle   */
        &compCode,              /* Completion code     */
        &reason);               /* Reason code         */
```

- V 9.3.5 Chcete-li dodat token ověření z aplikace Java , postupujte takto:

  Aplikace používající IBM MQ classes for JMS/Jakarta Messaging mohou poskytnout token prostřednictvím libovolné metody `createContext`nebo `createConnection` , která používá jméno uživatele a heslo.

  Chcete-li poskytnout token ověření, postupujte takto:

  – **UserID** musí být nastaven buď na hodnotu null, nebo na prázdný řetězec, tj. bez mezer, " "
  – Token je poskytnut jako řetězec **Password** .

  Toto platí pro všechny implementace IBM MQ rozhraní `ConnectionFactory` .

  Lze použít buď explicitní formuláře parametrů, například `createContext`(String **userID**, String **password**), nebo implicitní verze parametrů, například `createContext`().

  Ve druhém případě musí být jako vlastnosti pro továrnu připojení nejprve poskytnuty prázdné vlastnosti **userID** a Token **Password** .

  Příklad kódu Java pro připojení ke správci front pomocí tokenu ověření:

```
// Obtain token from authentication provider here:

String myToken = "xxxxxxxxxxxxxxx";

// Acquire instance of an MQ connection Factory:

JmsFactoryFactory ff = JmsFactoryFactory.getInstance(WMQConstants.WMQ_PROVIDER);

JmsConnectionFactory cf = ff.createConnectionFactory();
```

```
// Configure any required CF properties here - e.g. MQ Channel details

// Connect to (and authenticate with) the queue manager:

context = cf.createContext(null, myToken); // NOTE - null userID indicates token being
provided
```

Pokud připojení selže s kódem příčiny MQRC_NOT_AUTHORIZED (2035) nebo MQRC_SECURITY_ERROR (2063), zkontrolujte protokol chyb správce front, zda neobsahuje chybovou zprávu, která obsahuje další informace o příčině selhání. Další nápovědu k diagnostice problémů s tokeny ověření naleznete v tématu Odstraňování problémů s tokeny ověření.

Výsledky

Aplikace je nyní připojena ke správci front. Zůstane připojen, dokud se neodpojí, a to i v případě, že tokenu, který byl použit k ověření, vyprší platnost. Pokud se aplikace odpojí od správce front a potřebuje se znovu připojit, může být nutné získat nový token ověření s pozdější dobou vypršení platnosti, než se bude moci znovu připojit.

Související úlohy

Konfigurace správce front pro přijetí **AuthTokens**

Související odkazy

Sekce AuthToken souboru `qm.ini`

MQCSP-parametry zabezpečení

Práce se zrušenými certifikáty

Digitální certifikáty mohou být odvolány certifikačním úřadem. V závislosti na platformě můžete zkontrolovat stav odvolání certifikátů pomocí protokolu OCSP nebo seznamů CRL na serverech LDAP.

Během navázání komunikace TLS se komunikující partneři navzájem ověřují pomocí digitálních certifikátů. Ověření může zahrnovat i kontrolu, zda je přijatý certifikát nadále důvěryhodný. Certifikační autority (CA) odvolávají certifikáty z různých důvodů, včetně:

- Vlastník se přesunul do jiné organizace
- Soukromý klíč již není tajný

Certifikační autority publikují odvolané osobní certifikáty v seznamu odvolaných certifikátů (CRL). Certifikáty CA, které byly odvolány, jsou publikovány v seznamu odvolaných oprávnění (ARL).

ALW Na platformách AIX, Linux, and Windows podpora zabezpečení SSL produktu IBM MQ kontroluje odvolané certifikáty pomocí protokolu OCSP (Online Certificate Status Protocol) nebo pomocí seznamů CRL a ARL na serverech LDAP (Lightweight Directory Access Protocol). Preferovaná metoda je OCSP.

Produkty IBM MQ classes for Java a IBM MQ classes for JMS nemohou používat informace OCSP v souboru s tabulkou definic kanálů klienta. Nicméně můžete OCSP nakonfigurovat podle popisu uvedeného v tématu Používání protokolu certifikátů online.

z/OS IBM i Na platformách IBM i a z/OS podpora SSL IBM MQ kontroluje odvolané certifikáty pomocí seznamů CRL a ARL pouze na serverech LDAP.

Další informace o certifikačních autoritách naleznete v části “digitální certifikáty” na stránce 13.

Kontrola OCSP/CRL

Kontrola protokolu OCSP (Online Certificate Status Protocol) /CRL (Certificate Revocation List) se provádí pro vzdálené příchozí certifikáty. Proces kontroluje celý řetězec od osobního certifikátu vzdáleného systému až po jeho kořenový certifikát.

Použití openSSL k ověření ověření OCSP

Pokud váš podnik používá k ověření protokolu OCSP protokol openSSL a poté se pokusíte použít připojení TLS systému IBM Global Security Kit (GSKit) , obdržíte varování o stavu Neznámý.

Je to proto, že všechny certifikáty v řetězu, kromě kořene, jsou kontrolovány produktem GSKit pro stav odvolání. Operace GSKit je v souladu s RFC 5280 a je popsána v GSKit zásadě důvěryhodnosti. Algoritmus GSKit se pokusí o všechny dostupné zdroje informací o odvolání, jak je popsáno v RFC 5280 a v zásadách důvěryhodnosti sady GSGSKitKit.

Jak funguje kontrola OCSP/CRL v produktu IBM MQ?

Produkt IBM MQ podporuje dva mechanizmy pro řízení chování při kontrole certifikátů vůči pojmenovaným koncovým bodům OCSP nebo CRL, a to buď v rozšíření certifikátu, nebo, jak je definováno v objektech AUTHINFO:

- Atributy **OCSPCheckExtensions**, **CDPCheckExtensions**a **OCSPAuthentication** sekce SSL souboru qm.inia
- Použití parametru SSLCRLNL správce front a konfigurací AUTHINFO OCSP a CRLLDAP. Další informace viz ALTER AUTHINFO a ALTER QMGR .

Upozornění:

Příkaz ALTER AUTHINFO s parametrem **AUTHTYPE(OCSP)** se nevztahuje na správce front IBM i nebo z/OS . Na těchto platformách však může být určena ke zkopírování do tabulky CCDT (Client Channel Definition Table) pro použití klientem.

Atributy **OCSPCheckExtensions** a **CDPCheckExtensions** sekce SSL řídí, zda produkt IBM MQ ověří certifikát vůči serveru OCSP nebo CRL, který je podrobně popsán v rozšíření AIA certifikátu.

Není-li tato volba povolena, není kontaktován server OCSP nebo CRL v rozšíření certifikátu.

Pokud jsou servery OCSP nebo CRL podrobně popsány prostřednictvím objektů AUTHINFO a jsou na ně odkazovány pomocí atributu SSLCRLNL **QMGR** , pak se produkt IBM MQ během zpracování odvolání certifikátu pokusí kontaktovat tyto servery.

Důležité: V seznamu názvů SSLCRLNL lze definovat pouze jeden objekt OCSP AUTHINFO.

Pokud:

Jsou nastaveny hodnoty **OCSPCheckExtensions**= NO a **CDPCheckExtensions**=*NO* a
V objektech AUTHINFO nejsou definovány žádné servery OCSP nebo CRL

nebyla provedena žádná kontrola odvolání certifikátu.

Při ověřování certifikátu pro jeho stav odvolání produkt IBM MQ kontaktuje servery OCSP nebo CRL uvedené v následujícím pořadí, je-li povoleno:

1. Server OCSP podrobně popsaný v objektu **AUTHTYPE(OCSP)** a odkazovaný v atributu SSLCRLNL **QMGR** .
2. Servery OCSP podrobně popsané v rozšíření AIA certifikátů, pokud **OCSPCheckExtensions**=*YES*.
3. Servery CRL podrobně popsané v rozšíření **CRLDistributionPoints** certifikátů, pokud **CDPCheckExtensions** =*YES*.
4. Všechny servery CRL podrobně popsané v objektech **AUTHINFO(CRLLDAP)** a odkazované v atributu SSLCRLNL **QMGR** .

Pokud při ověřování certifikátu server OCSP nebo server CRL vrátí definitivní odpověď REVOKED nebo VALID na dotaz na certifikát, neprovedou se žádné další kontroly a stav předloženého certifikátu se použije k určení, zda mu důvěřovat či nikoli.

Pokud server OCSP nebo server CRL vrátí výsledek UNKNOWN, zpracování pokračuje, dokud server OCSP nebo CRL nevrátí konečný výsledek, nebo dokud nejsou vyčerpány všechny volby.

Chování, zda je certifikát považován za odvolaný, pokud jeho stav nelze určit, se liší pro servery OCSP a CRL:

- Pro servery CRL platí, že pokud nelze získat žádný seznam CRL, je certifikát považován za `NOT_REVOKED`
- U serverů OCSP, pokud nelze získat stav odvolání z pojmenovaného serveru OCSP, je chování řízeno pomocí atributu **`OCSPAuthentication`** v sekci SSL souboru qm.ini .

  Tento atribut můžete nakonfigurovat tak, aby buď blokoval připojení, povolil připojení, nebo povolil připojení s varovnou zprávou.

V případě potřeby můžete použít atribut **`SSLHTTPProxyName`**=*string* v sekci SSL souborů qm.ini a mqclient.ini pro kontroly OCSP. Řetězec je buď název hostitele, nebo síťová adresa serveru proxy HTTP, který má produkt GSKit použít pro kontroly OCSP.

V souboru IBM MQ 9.1.5 můžete nastavit hodnotu **`OCSPTimeout`** v sekci SSL souborů `qm.ini` nebo `mqclient.ini` , která nastaví počet sekund čekání na odpovídací modul OCSP při provádění kontroly odvolání.

ALW Zrušené certifikáty and OCSP

Produkt IBM MQ zjišťuje, který odpovídací modul protokolu OCSP (Online Certificate Status Protocol) má použít, a zpracovává přijatou odezvu. V některých případech je nutné provést kroky, kterými zpřístupníte odpovídací modul OCSP.

Poznámka: Tyto informace platí pouze pro systémy IBM MQ na systému AIX, Linux, and Windows .

Chcete-li zkontrolovat stav odvolání digitálního certifikátu pomocí protokolu OCSP, produkt IBM MQ může pomocí dvou metod určit, který odpovídací modul OCSP se má kontaktovat:

- Pomocí rozšíření certifikátu AIA (AuthorityInfoAccess) v kontrolovaném certifikátu.
- Pomocí adresy URL zadané v objektu ověřovacích informací nebo určené aplikací klienta.

Adresa URL uvedená v objektu ověřovacích informací nebo v aplikaci klienta má přednost před adresou URL v rozšíření certifikátu AIA.

Nachází-li se adresa URL odpovídacího modulu OCSP za branou firewall, změňte konfiguraci brány firewall tak, aby k odpovídacímu modulu OCSP bylo možné přistupovat, nebo zřiďte server proxy pro OCSP. Název serveru proxy zadejte pomocí proměnné SSLHTTPProxyName v sekci SSL. V klientských systémech můžete název serveru proxy zadat také pomocí proměnné prostředí MQSSLPROXY. Další podrobnosti naleznete v souvisejících informacích.

Pokud vám nezáleží na tom, zda jsou certifikáty TLS zrušené, například proto, že pracujete v testovacím prostředí, můžete nastavit proměnnou OCSPCheckExtensions v sekci SSL na hodnotu NO. Pokud nastavíte tuto proměnnou, bude ignorováno rozšíření certifikátu AIA. V provozním prostředí, kde zřejmě nebudete chtít umožnit přístup uživatelům předkládajícím zrušené certifikáty, toto řešení pravděpodobně nebude přijatelné.

Volání za účelem získání přístupu k odpovídacímu modulu OCSP může vyvolat jeden z těchto tří výsledků:

Platný
Certifikát je platný.

Zrušený
Certifikát je zrušený.

Neznámý
Tento výsledek se může vyskytnout ze tří různých příčin:

- Produkt IBM MQ nezískal přístup k odpovídacímu modulu OCSP.
- Odpovídací modul OCSP odeslal odezvu, ale produktu IBM MQ se nepodařilo ověřit digitální podpis této odezvy.
- Odpovídací modul OCSP odeslal odezvu s informací, že nemá k dispozici žádná data o odvolání daného certifikátu.

Obdrží-li produkt IBM MQ výsledek protokolu OCSP Neznámý, jeho chování bude záviset na nastavení atributu OCSPAuthentication. Pro správce front je tento atribut zadržen v jednom z následujících umístění:

- Linux AIX V sekci SSL souboru qm.ini na systému AIX and Linux.
- Windows V registru Windows .

Tento atribut lze nastavit pomocí IBM MQ Explorer. Pro klienty je atribut zadržen v sekci SSL konfiguračního souboru klienta.

Je-li přijat výsledek Neznámý a atribut OCSPAuthentication je nastaven na hodnotu REQUIRED (výchozí hodnota), produkt IBM MQ připojení odmítne a vydá chybovou zprávu typu AMQ9716. Jsou-li povoleny zprávy o událostech správce front SSL, dojde k vygenerování zprávy o události SSL typu MQRC_CHANNEL_SSL_ERROR s atributem ReasonQualifier nastaveným na hodnotu MQRQ_SSL_HANDSHAKE_ERROR.

Je-li přijat výsledek Neznámý a atribut OCSPAuthentication je nastaven na hodnotu OPTIONAL, produkt IBM MQ umožní spuštění kanálu SSL a nebudou vygenerována žádná varování ani zprávy o událostech SSL.

Je-li přijat výsledek Neznámý a atribut OCSPAuthentication je nastaven na hodnotu WARN, kanál SSL se spustí, ale produkt IBM MQ zapíše do protokolu chyb varovnou zprávu typu AMQ9717. Jsou-li povoleny zprávy o událostech správce front SSL, dojde k vygenerování zprávy o události SSL typu MQRC_CHANNEL_SSL_WARNING s atributem ReasonQualifier nastaveným na hodnotu MQRQ_SSL_UNKNOWN_REVOCATION.

Digitální podepisování odezev OCSP

Odpovídací modul OCSP může své odezvy podepisovat jedním ze tří způsobů. Váš odpovídací modul vás informuje o tom, která metoda je použita.

- Odezva OCSP může být digitálně podepsána s použitím téhož certifikátu CA, který byl použit k vystavení kontrolovaného certifikátu. V tomto případě nemusíte nastavovat žádný další certifikát; kroky, které jste již provedli k vytvoření připojitelnosti TLS, jsou dostatečné k ověření odezvy OCSP.
- Odezva OCSP může být digitálně podepsána s použitím jiného certifikátu podepsaného stejnou certifikační autoritou (CA), která vydala kontrolovaný certifikát. Podpisový certifikát je v tomto případě odeslán v jednom toku s odezvou OCSP. Certifikát přenášený tokem z odpovídacího modulu OCSP musí mít nastavené rozšíření použití rozšířeného klíče na hodnotu id-kp-OCSPSigning, aby mu bylo možné pro tento účel důvěřovat. Vzhledem k tomu, že odpověď OCSP je odeslána s certifikátem, který ji podepsal (a tento certifikát je podepsán certifikační autoritou, která je již důvěryhodná pro konektivitu TLS), není vyžadováno žádné další nastavení certifikátu.
- Odezva OCSP může být digitálně podepsána s použitím jiného certifikátu, který přímo nesouvisí s kontrolovaným certifikátem. V takovém případě je odezva OCSP podepsána certifikátem vydaným samotným odpovídacím modulem OCSP. Musíte přidat kopii certifikátu odpovídacího modulu OCSP do databáze klíčů klienta nebo správce front, který provádí kontrolu OCSP. Viz “Přidání certifikátu CA nebo veřejné části certifikátu podepsaného držitelem do úložiště klíčů v systému AIX, Linux, and Windows” na stránce 318. Přidávaný certifikát CA je standardně přidán jako důvěryhodný kořenový certifikát, což je v tomto kontextu povinné nastavení. Není-li tento certifikát přidán, produkt IBM MQ nemůže ověřit digitální podpis v odpovědi OCSP a výsledkem kontroly OCSP je neznámý výsledek, což může v závislosti na hodnotě OCSPAuthentication způsobit zavření kanálu produktem IBM MQ .

Online protokol OCSP (Certificate Status Protocol) v Java a JMS klientských aplikacích

Vzhledem k omezení rozhraní Java API může produkt IBM MQ používat kontrolu odvolání certifikátů OCSP (Online Certificate Status Protocol) pro zabezpečené sokety TLS pouze v případě, že je protokol OCSP povolen pro celý proces prostředí JVM (Java Virtual Machine). K dispozici jsou dva způsoby povolení OCSP pro všechny zabezpečené sokety v prostředí JVM:

- Upravte soubor JRE java.security zahrnutím nastavení konfigurace OCSP, jež jsou uvedena v tabulce 1, a restartujte aplikaci.
- Použijte java.security.Security.setProperty() Rozhraní API, s výhradou platné zásady Java Security Manager.

Přinejmenším musíte zadat jednu z hodnot ocsp.enable a ocsp.responderURL.

Název vlastnosti	**Popis**
ocsp.enable	Tato vlastnost má hodnotu `true` nebo `false`. Je-li použita hodnota `true`, je kontrola OCSP povolena při kontrole odvolání certifikátu. Je-li použita hodnota `false` nebo není-li vlastnost nastavena vůbec, je kontrola OCSP vypnuta.
ocsp.responderURL	Tato vlastnost nese hodnotu, jež odpovídá adrese URL, která určuje umístění odpovídacího modulu OCSP. Příklad: `ocsp.responderURL=http://ocsp.example.net:80`. Při výchozím nastavení se umístění odpovídacího modulu OCSP určuje implicitně z ověřovaného certifikátu. Vlastnost se používá, pokud v certifikátu chybí rozšíření Authority Information Access (definované v dokumentu RFC 3280) nebo pokud vyžaduje potlačení.
ocsp.responderCertSubjectName	Tato vlastnost nese hodnotu, jež určuje název subjektu certifikátu odpovídacího modulu OCSP. Příklad: `ocsp.responderCertSubjectName="CN=OCSP Responder, O=XYZ Corp"`. Při výchozím nastavení certifikát odpovídacího modulu OCSP má vydavatele, který vydal ověřovaný certifikát. Tato vlastnost identifikuje certifikát odpovídacího modulu OCSP v případě, že nelze použít výchozí hodnotu. Jeho hodnota je řetězec úplného názvu (definovaný RFC 2253), který identifikuje certifikát v sadě certifikátů poskytnutých během ověřování cest certifikátu. V případech, kdy samotný název subjektu nepostačuje k jedinečné identifikaci certifikátu, musejí být místo něj použity obě tyto vlastnosti: ocsp.responderCertIssuerName a ocsp.responderCertSerialNumber. Je-li tato vlastnost nastavena, budou vlastnosti ocsp.responderCertIssuerName a ocsp.responderCertSerialNumber ignorovány.
ocsp.responderCertIssuerName	Tato vlastnost nese hodnotu odpovídající názvu vydavatele certifikátu odpovídacího modulu OCSP. Příklad: `ocsp.responderCertIssuerName="CN=Enterprise CA, O=XYZ Corp"`. Při výchozím nastavení certifikát odpovídacího modulu OCSP má vydavatele, který vydal ověřovaný certifikát. Tato vlastnost identifikuje certifikát odpovídacího modulu OCSP v případě, že nelze použít výchozí hodnotu. Jeho hodnota je řetězec úplného názvu (definovaný RFC 2253), který identifikuje certifikát v sadě certifikátů poskytnutých během ověřování cest certifikátu. Je-li tato vlastnost nastavena, musí být nastavena rovněž vlastnost ocsp.responderCertSerialNumber. Tato vlastnost je ignorována, je-li nastavena vlastnost ocsp.responderCertSubjectName.
ocsp.responderCertSerialNumber	Tato vlastnost nese hodnotu, jež je sériovým číslem certifikátu odpovídacího modulu OCSP. Příklad: `ocsp.responderCertSerialNumber=2A:FF:00`. Při výchozím nastavení certifikát odpovídacího modulu OCSP má vydavatele, který vydal ověřovaný certifikát. Tato vlastnost identifikuje certifikát odpovídacího modulu OCSP v případě, že nelze použít výchozí hodnotu. Tato hodnota je řetězec hexadecimálních číslic (jako oddělovače mohou být použity dvojtečka a mezera) identifikující certifikát v sadě certifikátů poskytnutých během

Název vlastnosti	Popis
	ověřování cest certifikátu. Je-li tato vlastnost nastavena, musí být nastavena rovněž vlastnost ocsp.responderCertIssuerName. Tato vlastnost je ignorována, je-li nastavena vlastnost ocsp.responderCertSubjectName.

Dříve než povolíte OCSP tímto způsobem, zvažte tyto aspekty:

- Nastavení konfigurace OCSP ovlivňují všechny zabezpečené sokety v procesu JVM. V některých případech může mít tato konfigurace nežádoucí vedlejší účinky, pokud je prostředí JVM sdíleno s jiným kódem aplikace, který používá zabezpečené sokety TLS. Zajistěte, aby zvolená konfigurace OCSP byla vhodná pro všechny aplikace, jež běží ve stejném prostředí JVM.
- Při použití opravy pro vaše prostředí JRE může dojít k přepsání souboru java.security. Při použití prozatímních oprav Java a údržby produktu buďte opatrní, abyste se vyvarovali přepsání souboru java.security . Po použití balíčku údržby může být nezbytné znovu provést vlastní změny v souboru java.security. Z tohoto důvodu může být výhodnější provést nastavení konfigurace OCSP prostřednictvím rozhraní API java.security.Security.setProperty().
- Povolení kontroly OCSP se projeví pouze v případě, že je povolena rovněž kontrola odvolání. Kontrola odvolání se povoluje metodou `PKIXParameters.setRevocationEnabled()`.
- Používáte-li zachytávač AMS Java Interceptor popsaný v tématu Povolení kontroly OCSP v nativních zachytávačích, vyvarujte se použití konfigurace java.security OCSP, která je v konfliktu s konfigurací AMS OCSP v konfiguračním souboru úložiště klíčů.

Práce se seznamy odvolaných certifikátů a seznamy odvolaných oprávnění

Podpora systému IBM MQ pro seznamy CRL a ARL se liší podle platformy.

Podpora CRL a ARL na každé platformě je následující:

- V systému z/OSsystémové zabezpečení SSL podporuje seznamy CRL a seznamy ARL uložené na serverech LDAP produktem Tivoli Public Key Infrastructure.
- Na jiných platformách podpora CRL a ARL vyhovuje doporučením profilu CRL PKIX X.509 V2 .

Produkt IBM MQ udržuje mezipaměť seznamů CRL a ARL, ke kterým bylo přistupováno během předchozích 12 hodin.

Když správce front nebo produkt IBM MQ MQI client obdrží certifikát, zkontroluje seznam CRL, aby potvrdil, že je certifikát stále platný. IBM MQ nejprve zkontroluje mezipaměť, pokud existuje. Pokud seznam CRL není v mezipaměti, produkt IBM MQ zjišťuje umístění serveru CRL LDAP v pořadí, v jakém se vyskytují v seznamu názvů objektů ověřovacích informací určeném atributem *SSLCRLNL* , dokud produkt IBM MQ nenalezne dostupný seznam CRL. Není-li seznam názvů zadán nebo je-li zadán s prázdnou hodnotou, nebudou seznamy CRL kontrolovány.

Nastavení serverů LDAP

Nakonfigurujte strukturu stromu informací o adresáři LDAP tak, aby odrážela hierarchii rozlišujících názvů certifikačních autorit. Toto proveďte pomocí souborů formátu výměny dat LDAP.

Nakonfigurujte strukturu DIT (Directory Information Tree) LDAP tak, aby používala hierarchii odpovídající rozlišujícím názvům certifikačních autorit, které vydávají certifikáty a seznamy CRL. Strukturu DIT můžete nastavit pomocí souboru, který používá LDIF (LDAP Data Interchange Format). K aktualizaci adresáře můžete také použít soubory LDIF.

Soubory LDIF jsou textové soubory ASCII, které obsahují informace požadované k definování objektů v adresáři LDAP. Soubory LDIF obsahují jednu nebo více položek, z nichž každá obsahuje rozlišující název, alespoň jednu definici třídy objektů a volitelně více definic atributů.

Atribut `certificateRevocationList;binary` obsahuje seznam odvolaných uživatelských certifikátů v binární podobě. Atribut `authorityRevocationList;binary` obsahuje binární seznam certifikátů CA, které byly odvolány. Pro použití s protokolem IBM MQ TLS musí binární data pro tyto atributy odpovídat

formátu DER (Definitivní pravidla kódování). Další informace o souborech LDIF naleznete v dokumentaci dodané se serverem LDAP.

Obrázek 20 na stránce 365 zobrazuje ukázkový soubor LDIF, který můžete vytvořit jako vstup pro server LDAP pro načtení seznamů CRL a ARL vydaných CA1, což je imaginární certifikační autorita s rozlišujícím názvem "CN=CA1, OU=Test, O=IBM, C=GB", nastavená testovací organizací v rámci produktu IBM.

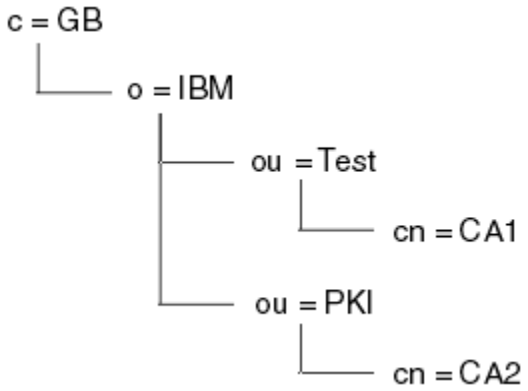
```
dn: o=IBM, c=GB
o: IBM
objectclass: top
objectclass: organization

dn: ou=Test, o=IBM, c=GB
ou: Test
objectclass: organizationalUnit

dn: cn=CA1, ou=Test, o=IBM, c=GB
cn: CA1
objectclass: cRLDistributionPoint
objectclass: certificateAuthority
authorityRevocationList;binary:: (DER format data)
certificateRevocationList;binary:: (DER format data)
caCertificate;binary:: (DER format data)
```

Obrázek 20. Ukázkový soubor LDIF pro certifikační autoritu. To se může lišit od implementace k implementaci.

Obrázek 21 na stránce 365 ukazuje strukturu DIT, kterou váš server LDAP vytvoří, když načtete ukázkový soubor LDIF zobrazený v souboru Obrázek 20 na stránce 365 spolu s podobným souborem pro CA2, imaginární certifikační autoritu nastavenou organizací PKI, také v rámci IBM.



Obrázek 21. Příklad struktury stromu informací o adresáři LDAP

Produkt IBM MQ kontroluje seznamy CRL i seznamy ARL.

Poznámka: Ujistěte se, že seznam přístupových práv pro váš server LDAP umožňuje oprávněným uživatelům číst, vyhledávat a porovnávat položky obsahující seznamy CRL a ARL. Produkt IBM MQ přistupuje k serveru LDAP pomocí vlastností LDAPUSER a LDAPPWD objektu AUTHINFO.

Konfigurace a aktualizace serverů LDAP
Pomocí této procedury nakonfigurujete nebo aktualizujete server LDAP.

1. Získejte seznamy CRL a ARL ve formátu DER od vaší certifikační autority nebo autorit.
2. Pomocí textového editoru nebo nástroje dodaného se serverem LDAP vytvořte jeden nebo více souborů LDIF, které obsahují rozlišující název CA a požadované definice tříd objektů. Zkopírujte data formátu DER do souboru LDIF jako hodnoty buď atributu `certificateRevocationList;binary` pro seznamy CRL, nebo atributu `authorityRevocationList;binary` pro seznamy ARL, nebo obojí.
3. Spusťte server LDAP.

4. Přidejte položky ze souboru nebo souborů LDIF, které jste vytvořili v kroku “2” na stránce 365.

Po nakonfigurování serveru LDAP CRL zkontrolujte, zda je správně nastaven. Nejprve zkuste použít certifikát, který není v kanálu odvolán, a zkontrolujte, zda je kanál správně spuštěn. Poté použijte odvolaný certifikát a zkontrolujte, zda se kanál nedaří spustit.

Často získávat aktualizované seznamy CRL od certifikačních autorit. Zvažte tuto možnost na svých serverech LDAP každých 12 hodin.

Přístup k seznamům CRL a ARL pomocí správce front

Správce front je přidružen k jednomu nebo více objektům ověřovacích informací, které obsahují adresu serveru LDAP CRL. IBM i IBM MQ on IBM i se chová odlišně od ostatních platforem.

Všimněte si, že v této části se informace o seznamech odvolaných certifikátů (CRL) vztahují také na seznamy odvolaných certifikátů (ARL).

Sdělte správci front, jak má přistupovat k seznamům CRL, zadáním objektů ověřovacích informací pro správce front, z nichž každý obsahuje adresu serveru LDAP CRL. Objekty ověřovacích informací jsou uloženy v seznamu názvů, který je uveden v atributu správce front *SSLCRLNL* .

V následujícím příkladu se k určení parametrů používá MQSC:

1. Definujte objekty ověřovacích informací pomocí příkazu DEFINE AUTHINFO MQSC s parametrem AUTHTYPE nastaveným na hodnotu CRLLDAP. IBM i V systému IBM imůžete také použít CL příkaz CRTMQMAUTI.

   Hodnota CRLLDAP pro parametr AUTHTYPE označuje, že k seznamům CRL se přistupuje na serverech LDAP. Každý objekt ověřovacích informací s typem CRLLDAP, který vytvoříte, obsahuje adresu serveru LDAP. Máte-li více než jeden objekt ověřovacích informací, musí servery LDAP, na které odkazují, obsahovat identické informace. To zajišťuje kontinuitu služby v případě selhání jednoho nebo více serverů LDAP.

   z/OS Dále, pouze v systému z/OS , musí být všechny servery LDAP přístupné pomocí stejného ID uživatele a hesla. Použité ID uživatele a heslo jsou uvedeny v prvním objektu AUTHINFO v seznamu názvů.

   Na všech platformách je ID uživatele a heslo odesláno na server LDAP bez šifrování.
2. Pomocí příkazu DEFINE NAMELIST MQSC definujte seznam názvů pro názvy objektů ověřovacích informací. z/OS V systému z/OSse ujistěte, že atribut seznamu názvů NLTYPE je nastaven na AUTHINFO.
3. Pomocí příkazu ALTER QMGR MQSC zadejte do správce front seznam názvů. Příklad:

   ```
   ALTER QMGR SSLCRLNL(sslcrlnlname)
   ```

   kde `sslcrlnlname` je seznam názvů objektů ověřovacích informací.

   Tento příkaz nastaví atribut správce front s názvem *SSLCRLNL*. Počáteční hodnota správce front pro tento atribut je prázdná.

IBM i V systému IBM imůžete zadat objekty ověřovacích informací, ale správce front nepoužívá objekty ověřovacích informací ani seznam názvů objektů ověřovacích informací. Pouze klienti IBM MQ , kteří používají tabulku připojení klienta generovanou správcem front IBM i , používají ověřovací informace určené pro daného správce front IBM i . Atribut správce front *SSLCRLNL* v systému IBM i určuje, jaké ověřovací informace klienti používají. Informace o tom, jak správce front IBM i přistupovat k seznamům CRL, naleznete v části “Přístup k seznamům CRL a ARL na systému IBM i” na stránce 367 .

Můžete přidat až 10 připojení k alternativním serverům LDAP do seznamu názvů, abyste zajistili kontinuitu služby, pokud jeden nebo více serverů LDAP selže. Všimněte si, že servery LDAP musí obsahovat identické informace.

IBM i *Přístup k seznamům CRL a ARL na systému IBM i*

Pomocí této procedury získáte přístup k seznamům CRL nebo ARL v systému IBM i.

Všimněte si, že v této části se informace o seznamech odvolaných certifikátů (CRL) vztahují také na seznamy odvolaných certifikátů (ARL).

Chcete-li nastavit umístění seznamu CRL pro specifický certifikát v systému IBM i, postupujte takto:

1. Přistupte k rozhraní DCM, jak je popsáno v tématu "Přístup k produktu DCM" na stránce 276.
2. V kategorii úloh **Spravovat umístění CRL** na navigačním panelu klepněte na volbu **Přidat umístění CRL**. V rámci úlohy se zobrazí stránka Spravovat umístění CRL.
3. Do pole **Název umístění CRL** zadejte název umístění CRL, například `LDAP Server #1`.
4. Do pole **Server LDAP** zadejte název serveru LDAP.
5. V poli **Použít SSL (Secure Sockets Layer)** vyberte volbu **Ano** , chcete-li se připojit k serveru LDAP pomocí TLS. Jinak vyberte volbu **Ne**.
6. Do pole **Číslo portu** zadejte číslo portu pro server LDAP, například 389.
7. Pokud váš server LDAP neumožňuje anonymním uživatelům dotazovat se na adresář, zadejte rozlišující název přihlášení pro server do pole **Rozlišující název přihlášení** .
8. Klepněte na tlačítko **OK**. Produkt DCM vás informuje, že vytvořil umístění CRL.
9. V navigačním panelu klepněte na volbu **Vybrat úložiště certifikátů**. V rámci úlohy se zobrazí stránka Vybrat úložiště certifikátů.
10. Označte zaškrtávací políčko **Jiná systémová paměť certifikátů** a klepněte na tlačítko **Pokračovat**. Zobrazí se stránka Úložiště certifikátů a heslo.
11. Do pole **Cesta a název souboru úložiště certifikátů** zadejte cestu IFS a název souboru, který jste nastavili při "Vytvoření úložiště certifikátů v systému IBM i" na stránce 279.
12. Zadejte heslo do pole **Heslo úložiště certifikátů** . Klepněte na tlačítko **Pokračovat**. V rámci úlohy se zobrazí stránka Aktuální úložiště certifikátů.
13. V kategorii úloh **Spravovat certifikáty** v navigačním panelu klepněte na volbu **Aktualizovat přiřazení umístění CRL**. Stránka Přiřazení umístění CRL se zobrazí v rámci úlohy.
14. Vyberte přepínač pro certifikát CA, ke kterému chcete přiřadit umístění seznamu CRL. Klepněte na volbu **Aktualizovat přiřazení umístění CRL**. V rámci úlohy se zobrazí stránka Aktualizovat přiřazení umístění CRL.
15. Vyberte přepínač pro umístění CRL, které chcete přiřadit k certifikátu. Klepněte na volbu **Aktualizovat přiřazení**. Produkt DCM vás informuje, že aktualizoval přiřazení.

Všimněte si, že produkt DCM vám umožňuje přiřadit jiný server LDAP podle certifikační autority.

Přístup k seznamům CRL a ARL pomocí IBM MQ Explorer

Pomocí funkce IBM MQ Explorer můžete správci front sdělit, jak má přistupovat k seznamům CRL.

Všimněte si, že v této části se informace o seznamech odvolaných certifikátů (CRL) vztahují také na seznamy odvolaných certifikátů (ARL).

Chcete-li nastavit připojení LDAP k seznamu CRL, postupujte takto:

1. Ujistěte se, že jste spustili správce front.
2. Klepněte pravým tlačítkem myši na složku **Ověřovací informace** a klepněte na volbu **Nový-> Ověřovací informace**. V listu vlastností, který se otevře:
   a. Na první stránce **Vytvořit ověřovací informace**zadejte název objektu CRL (LDAP).
   b. Na stránce **Obecné** v části **Změnit vlastnosti**vyberte typ připojení. Volitelně můžete zadat popis.
   c. Vyberte stránku **CRL (LDAP)** v části **Změnit vlastnosti**.
   d. Zadejte název serveru LDAP jako název sítě nebo adresu IP.
   e. Pokud server vyžaduje přihlašovací údaje, zadejte ID uživatele a v případě potřeby heslo.
   f. Klepněte na tlačítko **OK**.

3. Klepněte pravým tlačítkem myši na složku Seznam názvů a klepněte na volbu **Nový-> Seznam názvů**. V listu vlastností, který se otevře:
   a. Zadejte název seznamu názvů.
   b. Přidejte název objektu CRL (LDAP) (z kroku “2.a” na stránce 367) do seznamu.
   c. Klepněte na tlačítko **OK**.
4. Klepněte pravým tlačítkem myši na správce front, vyberte volbu **Vlastnosti**a vyberte stránku **SSL** :
   a. Zaškrtněte políčko **Zkontrolovat certifikáty přijaté tímto správcem front pro seznamy odvolaných certifikátů** .
   b. Zadejte název seznamu názvů (z kroku “3.a” na stránce 368). v poli **Seznam názvů CRL** .

Přístup k seznamům CRL a ARL pomocí IBM MQ MQI client

Máte tři volby pro určení serverů LDAP, které uchovávají seznamy CRL pro kontrolu pomocí IBM MQ MQI client.

Všimněte si, že v této části se informace o seznamech odvolaných certifikátů (CRL) vztahují také na seznamy odvolaných certifikátů (ARL).

Tři způsoby určení serverů LDAP jsou následující:

- Použití tabulky definic kanálů
- Použití struktury voleb konfigurace SSL MQSCO ve volání MQCONNX
- Použití Active Directory (na systémech Windows s podporou Active Directory)

Další podrobnosti viz související informace.

Můžete zahrnout až 10 připojení k alternativním serverům LDAP, abyste zajistili kontinuitu služby, pokud jeden nebo více serverů LDAP selže. Všimněte si, že servery LDAP musí obsahovat identické informace.

K seznamům CRL LDAP nelze přistupovat z kanálu IBM MQ MQI client spuštěného na platformě Linux (zSeries).

Umístění odpovídacího modulu OCSP a serverů LDAP, které obsahují seznamy CRL.
V systému IBM MQ MQI client můžete určit umístění odpovídacího modulu OCSP a serverů LDAP (Lightweight Directory Access Protocol), které obsahují seznamy odvolaných certifikátů (CRL).

Tato umístění můžete zadat třemi způsoby, popsanými zde v pořadí podle klesající priority.

IBM i Informace o systému IBM inaleznete v tématu Přístup k seznamům CRL a ARL v systému IBM i.

Když aplikace IBM MQ MQI client vydá volání MQCONNX

Můžete určit odpovídací modul OCSP nebo server LDAP, který bude při volání **MQCONNX** zadržovat seznamy CRL.

Při volání **MQCONNX** může struktura voleb připojení MQCNO odkazovat na strukturu voleb konfigurace SSL MQSCO. Struktura MQSCO může odkazovat na jednu nebo více struktur záznamu ověřovacích informací, MQAIR. Každá struktura MQAIR obsahuje všechny informace, které produkt IBM MQ MQI client vyžaduje pro přístup k odpovídacímu modulu OCSP nebo serveru LDAP, který obsahuje seznamy CRL. Jedním z polí ve struktuře MQAIR je například URL , na které lze kontaktovat odpovídací modul. Další informace o struktuře MQAIR viz MQAIR-záznam ověřovacích informací.

Použití tabulky definic kanálů klienta (ccdt) pro přístup k odpovídacímu modulu OCSP nebo serverům LDAP

Aby mohl produkt IBM MQ MQI client přistupovat k odpovídacímu modulu OCSP nebo serverům LDAP, které obsahují seznamy CRL, zahrňte atributy jednoho nebo více objektů ověřovacích informací do tabulky definic kanálů klienta.

Ve správci front serveru můžete definovat jeden nebo více objektů ověřovacích informací. Atributy objektu ověřování obsahují všechny informace, které jsou nezbytné pro přístup k odpovídacímu modulu OCSP (na platformách, kde je podporován protokol OCSP) nebo k serveru LDAP, který uchovává seznamy CRL. Jeden z atributů uvádí URLodpovídacího modulu OCSP, jiný uvádí adresu hostitele nebo adresu IP systému, na kterém je spuštěn server LDAP.

z/OS IBM i Objekt ověřovacích informací s parametrem AUTHTYPE (OCSP) nelze použít pro použití ve správcích front IBM i nebo z/OS , lze jej však určit na těchto platformách, které mají být zkopírovány do tabulky CCDT (Client Channel Definition Table) pro použití klientem.

Chcete-li povolit produktu IBM MQ MQI client přístup k odpovídacímu modulu OCSP nebo serverům LDAP, které obsahují seznamy CRL, atributy jednoho nebo více objektů ověřovacích informací lze zahrnout do tabulky definic kanálů klienta. Tyto atributy můžete zahrnout jedním z následujících způsobů:

Multi

Na platformách serveru AIX, Linux, IBM ia Windows

Můžete definovat seznam názvů, který obsahuje názvy jednoho nebo více objektů ověřovacích informací. Poté můžete nastavit atribut správce front **SSLCRLNL**na název tohoto seznamu názvů.

Používáte-li seznamy CRL, lze konfigurovat více serverů LDAP tak, aby poskytovaly vyšší dostupnost. Záměrem je, aby každý server LDAP uchovoval stejné seznamy CRL. Pokud je jeden server LDAP nedostupný, když je požadován, IBM MQ MQI client se může pokusit o přístup k jinému serveru.

Atributy objektů ověřovacích informací identifikovaných pomocí seznamu názvů jsou zde souhrnně označovány jako *umístění odvolání certifikátu*. Nastavíte-li atribut správce front **SSLCRLNL**na název seznamu názvů, bude umístění odvolání certifikátu zkopírováno do tabulky definic kanálů klienta přidružené ke správci front. Pokud lze k tabulce CCDT přistupovat z klientského systému jako ke sdílenému souboru nebo pokud je tabulka CCDT zkopírována do klientského systému, může agent IBM MQ MQI client v tomto systému použít umístění odvolání certifikátu v tabulce CCDT pro přístup k odpovídacímu modulu OCSP nebo serverům LDAP, které obsahují seznamy CRL.

Dojde-li později ke změně umístění odvolaných certifikátů správce front, projeví se tato změna v tabulce CCDT přidružené ke správci front. Je-li atribut správce front **SSLCRLNL**nastaven na prázdnou hodnotu, bude umístění odvolání certifikátu odebráno z tabulky CCDT. Tyto změny se neprojeví v žádné kopii tabulky v klientském systému.

Pokud požadujete, aby se umístění odvolání certifikátu na straně klienta a serveru kanálu MQI lišilo, a správce front serveru je ten, který se používá k vytvoření umístění odvolání certifikátu, můžete to provést takto:

1. Ve správci front serveru vytvořte umístění odvolání certifikátu pro použití v klientském systému.
2. Zkopírujte tabulky CCDT obsahující umístění odvolání certifikátu do klientského systému.
3. Ve správci front serveru změňte umístění odvolání certifikátu na to, co je vyžadováno na konci serveru kanálu MQI.
4. Na klientském počítači můžete použít příkaz **runmqsc** s parametrem **-n** .

Multi

Na platformách klienta AIX, Linux, IBM ia Windows

Tabulky CCDT můžete sestavit v klientském počítači pomocí příkazu runmqsc s parametrem **-n** a objekty **DEFINE AUTHINFO** v souboru CCDT. Pořadí, ve kterém jsou objekty definovány, je pořadí, ve kterém jsou použity v souboru. Jakýkoli název, který můžete použít v objektu **DEFINE AUTHINFO** , nebude v souboru zachován. Pouze poziční čísla se používají, když **DISPLAY** objekty **AUTHINFO** v souboru CCDT.

Poznámka: Zadáte-li parametr **-n** , nesmíte zadat žádný jiný parametr.

Použití služby Active Directory v systému Windows

Windows

Na systémech Windows můžete použít řídicí příkaz **setmqcrl** k publikování aktuálních informací o seznamu CRL ve službě Active Directory.

Příkaz **setmqcrl** nepublikuje informace OCSP.

Informace o tomto příkazu a jeho syntaxi viz setmqcrl.

Přístup k seznamům CRL a ARL pomocí IBM MQ classes for Java a IBM MQ classes for JMS

IBM MQ classes for Java a IBM MQ classes for JMS přistupují k seznamům CRL odlišně od ostatních platforem.

Informace o práci se seznamy CRL a ARL s produktem IBM MQ classes for Javanaleznete v tématu Použití seznamů odvolaných certifikátů .

Informace o práci se seznamy CRL a ARL s produktem IBM MQ classes for JMSnaleznete v tématu Vlastnost objektu SSLCERTSTORES .

Manipulace s objekty ověřovacích informací

S objekty ověřovacích informací můžete manipulovat pomocí příkazů MQSC nebo PCF nebo pomocí konzoly IBM MQ Explorer.

Následující příkazy MQSC fungují na objektech ověřovacích informací:

- PŘEDEFINOVÁNO AUTHINFO
- ALTER AUTHINFO
- DELETE AUTHINFO (ODSTRANĚNÍ)
- ZOBRAZENÍ AUTHINFO

Úplný popis těchto příkazů naleznete v tématu Příkazy MQSC.

Následující příkazy PCF (Programmable Command Format) fungují na objektech ověřovacích informací:

- Vytvořit ověřovací informace
- Kopírovat ověřovací informace
- Změnit ověřovací informace
- Odstranit ověřovací informace
- Zjistit ověřovací informace
- Zjistit názvy ověřovacích informací

Úplný popis těchto příkazů naleznete v části Definice programovatelných formátů příkazů.

Na platformách, kde je k dispozici, můžete také použít IBM MQ Explorer.

Linux AIX Použití metody PAM (Pluggable Authentication Method)

Modul PAM můžete používat pouze na platformách AIX and Linux . Typický systém AIX nebo Linux má moduly PAM, které implementují tradiční mechanizmus ověřování; může však existovat více. Kromě základní úlohy ověřování hesel lze také vyvolat moduly PAM, které budou provádět další pravidla.

Konfigurační soubory definují, která metoda ověření se má použít pro každou aplikaci. Mezi vzorové aplikace patří standardní přihlášení terminálu, ftp a telnet.

Výhodou modulu PAM je, že aplikace nemusí vědět nebo se starat o to, jak je ID uživatele skutečně ověřováno. Dokud může aplikace poskytnout PAM správnou formu ověřovacích dat, mechanizmus za ním je transparentní.

Forma ověřovacích dat závisí na používaném systému. Například produkt IBM MQ získá heslo prostřednictvím parametrů, jako je struktura MQCSP použitá ve volání rozhraní API MQCONNX .

Důležité: Atribut **AUTHENMD** nelze nastavit, dokud nenainstalujete produkt IBM MQ 8.0.0 Fix Pack 3a poté nerestartujete správce front pomocí volby **-e CMDLEVEL=***úroveň 802* (v příkazu strmqm), která nastaví požadovanou úroveň příkazu.

Konfigurace systému pro použití PAM

Název služby používaný produktem IBM MQpři vyvolání modulu PAM je *ibmmq*.

Všimněte si, že instalace produktu IBM MQ se pokusí zachovat výchozí konfiguraci PAM, která povoluje připojení od uživatelů operačního systému na základě známých předvoleb pro různé operační systémy.

Administrátor systému však musí ověřit, zda jsou pravidla definovaná v souborech `/etc/pam.conf`nebo `/etc/pam.d/ibmmq`stále vhodná.

Autorizace přístupu k objektům

Tato část obsahuje informace o použití správce oprávnění k objektu a uživatelských programů kanálu pro řízení přístupu k objektům.

ALW Na systémech AIX, Linux, and Windows . řízení přístupu k objektům pomocí správce OAM (Object Authority Manager). Tato kolekce témat obsahuje informace o použití rozhraní příkazu pro modul OAM.

Tento oddíl také obsahuje kontrolní seznam, který můžete použít k určení úloh, které se mají provést pro použití zabezpečení na vašem systému na všech platformách, a pokyny pro udělení oprávnění uživatelům spravovat produkt IBM MQ a pracovat s objekty produktu IBM MQ .

Pokud dodané mechanizmy zabezpečení nevyhovují vašim potřebám, můžete vytvořit vlastní programy uživatelské procedury kanálu.

Určení, který uživatel se používá pro autorizaci

Oprávnění pro přístup k prostředkům jsou udělena skupinám, kterých je uživatel členem, nebo v určitých režimech přímo uživateli přidruženému k připojení. Během procesu připojení a zejména pro vzdálená (klientská) připojení může být tato identita změněna konfigurací správce front. Na této stránce jsou uvedeny různé funkce produktu IBM MQ a jejich volby konfigurace, které by mohly ovlivnit identitu připojující se aplikace, a pořadí, v jakém se tyto funkce projeví.

Funkce, které mohou upravit, který uživatel je adoptován

Různé funkce, které mohou nastavit, který uživatel by měl být autorizován, jsou následující:

Deklarovaný uživatel aplikace
Když produkt IBM MQspustí vzdálené připojení, odešle se uživateli operačního systému, který proces spouští, do přijímajícího správce front. Tento uživatel je odeslán, aby se ujistil, že pokud neexistuje žádná další konfigurace, která by upravila uživatele, existuje uživatel, kterého lze použít pro kontrolu autorizace.

Nedoporučuje se používat tohoto uživatele jako základ pro autorizaci, protože umožňuje připojení deklarovat svou identitu bez ověření na straně serveru. To může zahrnovat i administrativního uživatele ('mqm ').

Nastavení kanálu MCAUSER
Aplikace, které se připojují prostřednictvím vazeb sítě, tak činí pomocí definice kanálu IBM MQ . Definice kanálů podporují atribut **MCAUSER** , který lze použít k určení jiného uživatele, který má být použit pro autorizaci, namísto uživatele, který je aktivován připojovacími aplikacemi.

Ověření připojení ADOPTCTX
Aplikace mohou určit uživatele a heslo, které mají být odeslány správci front pro účely ověřování. Tato pověření jsou ověřena pomocí konfigurace, která je určena pro funkci Ověření připojení. Volba

ADOPTCTX pro ověření připojení řídí, zda by měl být uživatel použit pro autorizaci poté, co byl úspěšně ověřen. Je-li nastaveno na hodnotu YES, pak je uživatel, který je dodán pro ověření, převzat pro kontroly autorizace.

V 9.3.4 V produktu IBM MQ 9.3.4lze token dodat pro ověření, pokud je hodnota **ADOPTCTX** nastavena na YES, pak je uživatel převzat z nároků, které token obsahuje.

Záznam ověření kanálu MCAUSER
Během zpracování připojení se správce front pokusí najít záznam ověřování kanálu, který odpovídá připojení. Pokud je záznam ověřování kanálu shodný a jeho hodnota atributu **USERSRC** je nastavena na MAP, pak produkt IBM MQ změní uživatele použitého pro autorizace na hodnotu atributu **MCAUSER** .

Uživatelské procedury zabezpečení
Uživatelské procedury zabezpečení jsou vlastní funkce, které lze zapsat a volat během zpracování zabezpečení produktu IBM MQ . Je-li funkce volána, je dodávána s kopií struktury MQCD, která obsahuje několik polí souvisejících s uživatelem připojení, který bude použit pro kontroly autorizace. Uživatelské procedury zabezpečení mohou upravit tato pole a změnit uživatele, který bude autorizován.

pořadí priority

Následující tabulka zobrazuje pořadí priorit pro každou funkci zabezpečení popsanou v části "Funkce, které mohou upravit, který uživatel je adoptován" na stránce 371 když IBM MQ vybírá uživatele pro autorizaci. Pořadí je od nejnižšího k nejvyššímu, to znamená, že nastavení funkce zabezpečení uživatele na prvním řádku je potlačeno kterýkoliv z ostatních řádků.

Tabulka 71. Pořadí priorit pro funkce zabezpečení

Pořadí	**Funkce**
1 (nejnižší)	ID uplatněný aplikací
2	Atribut **MCAUSER** definice kanálu
3	Ověření připojení pomocí produktu **ADOPTCTX(YES)**
4	Záznamy ověření kanálu s **USERSRC(MAP)**
5 (nejvyšší)	Uživatelská procedura pro zabezpečení zprávy

Důsledky předčasného adopci

Záznamy ověření připojení a ověření kanálu poskytují volbu konfigurace, která řídí, kdy se provádí převzetí uživatele ověření připojení. Toto nastavení je označováno jako včasné přijetí. Je-li povoleno včasné převzetí, dojde k převzetí identity ověření připojení před zpracováním záznamů ověření kanálu (což znamená, že záznamy ověření kanálu přepíší jakékoli převzetí produktu **CONNAUTH**).

Je-li zakázáno, pořadí je obrácené-to znamená, že záznamy ověření kanálu jsou zpracovány před **CONNAUTH** adopcí. V této situaci má převzetí ověření připojení vyšší efektivní prioritu než záznamy ověření kanálu.

Výchozí nastavení pro včasné převzetí je `povoleno`.

ALW Řízení přístupu k objektům pomocí OAM na systému AIX, Linux, and Windows

Správce oprávnění k objektu (OAM) poskytuje příkazové rozhraní pro udělení a odvolání oprávnění k objektům IBM MQ .

K použití těchto příkazů musíte mít vhodnou autorizaci, jak je popsáno v tématu "Oprávnění ke správě IBM MQ v systému AIX, Linux, and Windows" na stránce 419. ID uživatelů, kteří jsou autorizováni pro

administraci produktu IBM MQ , mají oprávnění *superuživatele* ke správci front, což znamená, že jim nemusíte udělovat další oprávnění k vydávání požadavků nebo příkazů MQI.

Linux AIX Oprávnění založená na uživateli OAM na AIX and Linux

V systémech IBM MQ 8.0na systémech UNIX and Linux může správce oprávnění k objektu (OAM) používat autorizaci založenou na uživateli i autorizaci založenou na skupině.

Před IBM MQ 8.0jsou seznamy přístupových práv (ACL) v systému UNIX and Linux založeny pouze na skupinách. V systému IBM MQ 8.0jsou seznamy ACL založeny jak na ID uživatelů, tak na skupinách, a pro autorizaci můžete použít buď model založený na uživateli, nebo model založený na skupině nastavením atributu **SecurityPolicy** na odpovídající hodnotu, jak je popsáno v části Konfigurace instalovatelných služeb a Konfigurace sekcí autorizačních služeb v systému AIX and Linux.

Změny v chování pro produkt IBM MQ 8.0 a novější

V produktu IBM MQ 8.0při spuštění se zásadou založenou na uživateli některé příkazy vracejí jiné informace než předchozí verze produktu:

- Příkazy **dmpmqaut** a **dmpmqcfg** zobrazují záznamy založené na uživatelích, stejně jako ekvivalentní operace PCF.
- Modul plug-in OAM pro produkt IBM MQ Explorer zobrazuje záznamy založené na uživatelích a umožňuje úpravy založené na uživatelích.
- Funkce OAM **Inquire** vrací výsledky, které ukazují, že je schopna pracovat s uživatelem.

Použití atributu **-p** v příkazu **setmqaut** neudělí přístup všem uživatelům ve stejné primární skupině, když jsou v souboru `qm.ini` povoleny autorizace založené na uživateli, jak je popsáno v sekci Sekce služby souboru qm.ini.

Pokud začnete používat autorizaci založenou na uživatelích a máte mnoho uživatelů, pravděpodobně bude ve frontě AUTH uloženo více záznamů než u modelu založeného na skupinách a proces autorizace může trvat o něco déle než dříve, protože existuje více záznamů k ověření. Neočekává se, že by tento nárůst byl významný. V případě potřeby můžete použít kombinaci oprávnění uživatelů a skupin.

Aspekty migrace

Pokud pro existujícího správce front změníte model ze skupiny na uživatele, nedojde k žádnému okamžitému efektu. Autorizace, které již byly provedeny, jsou i nadále platné. Všichni uživatelé, kteří se připojují ke správci front, mají stejná oprávnění jako dříve: kombinace všech skupin, do kterých jejich ID patří. Když jsou pro ID uživatelů vydány nové příkazy **setmqaut** , projeví se okamžitě.

Pokud vytvoříte nového správce front se zásadou uživatele, bude mít tento správce front oprávnění pouze pro uživatele, který jej vytvořil (což je obvykle, ale ne nutně, ID uživatele `mqm`). Existují také oprávnění, která jsou automaticky udělena skupině `mqm` . Pokud však nemáte jako primární skupinu `mqm` , nebude skupina `mqm` zahrnuta do počáteční sady autorizací.

Pokud se přesunete z uživatele do zásady skupiny, autorizace založené na uživateli se automaticky neodstraní. Během kontroly oprávnění se však již nepoužívají. Před opětovným vrácením zásady uložte aktuální konfiguraci, změňte zásadu, restartujte správce front a poté znovu přehrajte skript. Vzhledem k tomu, že se nyní jedná o správce front založeného na skupinách, má to za následek, že se pravidla pro ID uživatelů ukládají na základě primární skupiny.

Související pojmy

správce oprávnění k objektu (OAM)

“Činitelé a skupiny na AIX, Linux, and Windows” na stránce 423

Činitelé mohou patřit do skupin. Udělíte-li přístup k prostředkům skupinám a nikoli jednotlivcům, můžete snížit požadovaný objem administrace. Seznamy přístupových práv (ACL) jsou založeny na skupinách i ID uživatelů.

Související odkazy

Sekce služby souboru qm.ini

crtmqm (vytvoření správce front), příkaz

ALW Udělení přístupu k objektu IBM MQ na AIX, Linux, and Windows

Pomocí řídicího příkazu **setmqaut** , příkazu **SET AUTHREC** MQSC nebo příkazu **MQCMD_SET_AUTH_REC** PCF udělte uživatelům a skupinám uživatelů přístup k objektům produktu IBM MQ . Všimněte si, že v systému IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Úplnou definici řídicího příkazu **setmqaut** a jeho syntaxi viz setmqaut.

Úplnou definici příkazu **SET AUTHREC** MQSC a jeho syntaxi naleznete v části SET AUTHREC.

Úplnou definici příkazu **MQCMD_SET_AUTH_REC** PCF a jeho syntaxi naleznete v části Nastavit záznam oprávnění.

Chcete-li použít tento příkaz, musí být spuštěn správce front. Když jste změnili přístup k činiteli, OAM změny okamžitě projeví.

Chcete-li uživatelům udělit přístup k objektu, musíte zadat:

- Název správce front, který vlastní objekty, se kterými pracujete. Pokud nezadáte název správce front, bude se předpokládat výchozí správce front.
- Název a typ objektu (jedinečně identifikovat objekt). Název zadáte jako *profil* ; je to buď explicitní název objektu, nebo generický název, včetně zástupných znaků. Podrobný popis generických profilů a použití zástupných znaků v nich viz “Použití generických profilů OAM na systému AIX, Linux, and Windows” na stránce 375.
- Jeden nebo více činitelů a názvů skupin, na které se oprávnění vztahuje.

  Pokud ID uživatele obsahuje mezery, uzavřete jej při použití tohoto příkazu do uvozovek. Na systémech Windows můžete ID uživatele kvalifikovat názvem domény. Pokud skutečné ID uživatele obsahuje symbol zavináč (@), nahraďte jej znakem @ @, aby se zobrazilo, že je součástí ID uživatele, nikoli oddělovačem mezi ID uživatele a názvem domény.
- Seznam oprávnění. Každá položka v seznamu uvádí typ přístupu, který má být danému objektu udělen (nebo od něj odvolán). Každá autorizace v seznamu je uvedena jako klíčové slovo s předponou se znaménkem plus (+) nebo znaménkem minus (-). Použijte znaménko plus pro přidání uvedené autorizace a znaménko minus pro odebrání autorizace. Mezi znaménkem + nebo-a klíčovým slovem nesmí být mezery.

  V jednom příkazu můžete zadat libovolný počet oprávnění. Například seznam autorizací, které umožňují uživateli nebo skupině vkládat zprávy do fronty a procházet je, ale zrušit přístup pro získání zpráv, je:

```
+browse -get +put
```

Příklady použití příkazu setmqaut

Následující příklady ukazují, jak pomocí příkazu `setmqaut` udělit a zrušit oprávnění k použití objektu:

```
setmqaut -m saturn.queue.manager -t queue -n RED.LOCAL.QUEUE
         -g groupa +browse -get +put
```

V tomto příkladu platí následující:

- `saturn.queue.manager` je název správce front.
- `queue` je typ objektu
- `RED.LOCAL.QUEUE` je název objektu
- `groupa` je identifikátor skupiny s autorizacemi, které se mají změnit.
- `+browse -get +put` je seznam oprávnění pro uvedenou frontu.

- Produkt +browse přidává autorizaci k procházení zpráv ve frontě (k vydání příkazu **MQGET** s volbou procházení).
- Produkt -get odebere autorizaci k získání (**MQGET**) zpráv z fronty.
- Produkt +put přidává autorizaci pro vložení (**MQPUT**) zpráv do fronty.

Následující příkaz odvolá oprávnění vložení do fronty MyQueue od činitele fvuser a od skupin groupa a groupb. Na systémech AIX and Linux tento příkaz také odvolá oprávnění vložení pro všechny činitele ve stejné primární skupině jako fvuser.

```
setmqaut -m saturn.queue.manager -t queue -n MyQueue -p fvuser
         -g groupa -g groupb -put
```

Použití příkazu setmqaut s jinou autorizační službou

Pokud místo OAM používáte vlastní autorizační službu, můžete zadat název této služby v příkazu **setmqaut** , abyste příkaz nasměrovali na tuto službu. Tento parametr musíte zadat, pokud je současně spuštěno více instalovatelných komponent; pokud tak neučiníte, provede se aktualizace první instalovatelné komponenty pro autorizační službu. Standardně se jedná o dodaný modul OAM.

Poznámky k použití příkazu SET AUTHREC

Seznam oprávnění pro přidání a seznam oprávnění pro odebrání se nesmí překrývat. Nemůžete například přidat oprávnění pro zobrazení a odebrat oprávnění pro zobrazení v jednom příkazu. Toto pravidlo platí i v případě, že jsou oprávnění vyjádřena různými volbami. Například následující příkaz se nezdaří, protože oprávnění DSP se překrývá s oprávněním ALLADM:

```
SET AUTHREC PROFILE(*) OBJTYPE(QUEUE) PRINCIPAL(PRINC01) AUTHADD(DSP) AUTHRMV(ALLADM)
```

Výjimkou z tohoto chování je oprávnění ALL. Následující příkaz nejprve přidá oprávnění ALL, a pak odebere oprávnění SETID:

```
SET AUTHREC PROFILE(*) OBJTYPE(QUEUE) PRINCIPAL(PRINC01) AUTHADD(ALL) AUTHRMV(SETID)
```

Následující příkaz nejprve odebere oprávnění ALL, a pak přidá oprávnění DSP:

```
SET AUTHREC PROFILE(*) OBJTYPE(QUEUE) PRINCIPAL(PRINC01) AUTHADD(DSP) AUTHRMV(ALL)
```

Bez ohledu na pořadí, v jakém je oprávnění v příkazu zadáno, se oprávnění ALL zpracuje vždy jako první.

ALW Použití generických profilů OAM na systému AIX, Linux, and Windows

Generické profily OAM se používají k nastavení oprávnění uživatele pro mnoho objektů v jedné operaci, spíše než k zadání samostatných příkazů **setmqaut** nebo **SET AUTHREC** pro každý jednotlivý objekt při jeho vytvoření. Všimněte si, že v systému IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Použití generických profilů v příkazech setmqaut nebo SET AUTHREC vám umožňuje nastavit generické oprávnění pro všechny objekty, které odpovídají tomuto profilu.

Tato kolekce témat podrobněji popisuje použití generických profilů.

Použití zástupných znaků v profilech OAM

Profil je generický použitím speciálních znaků (zástupných znaků) v názvu profilu. Zástupný znak otazník (?) například odpovídá libovolnému jednotlivému znaku v názvu. Pokud tedy zadáte hodnotu ABC . ?EF, bude autorizace, kterou jste udělili tomuto profilu, platit pro všechny objekty s názvy ABC . DEF, ABC . CEF, ABC . BEFatd.

K dispozici jsou následující zástupné znaky:

?

Otazník (?) zastupuje libovolný jeden znak. Například `AB.?D` platí pro objekty `AB.CD`, `AB.EDa AB.FD`.

*****

Použijte hvězdičku (*) jako:

- *Kvalifikátor* v názvu profilu tak, aby odpovídal libovolnému kvalifikátoru v názvu objektu. Kvalifikátor je část názvu objektu oddělená tečkou. Název objektu `ABC.DEF.GHI` se například skládá z kvalifikátorů `ABC`, `DEF` a `GHI`.

  Například `ABC.*.JKL` platí pro objekty `ABC.DEF.JKLa ABC.GHI.JKL`. (Všimněte si, že se **nevztahuje** na `ABC.JKL` ; * použité v tomto kontextu vždy označuje jeden kvalifikátor.)
- Znak v kvalifikátoru v názvu profilu, který odpovídá žádnému nebo více znakům v kvalifikátoru v názvu objektu.

  Například `ABC.DE*.JKL` platí pro objekty `ABC.DE.JKL`, `ABC.DEF.JKLa ABC.DEGH.JKL`.

******

Použijte dvojitou hvězdičku (**) **jednou** v názvu profilu jako:

- Celý název profilu, který má odpovídat všem názvům objektů. Pokud například použijete produkt `-t prcs` k identifikaci procesů a poté použijete ** jako název profilu, změníte oprávnění pro všechny procesy.
- Jako počáteční, střední nebo koncový kvalifikátor v názvu profilu odpovídá žádnému nebo více kvalifikátorům v názvu objektu. Například `**.ABC` identifikuje všechny objekty s konečným kvalifikátorem ABC.

Jako úplný kvalifikátor můžete použít pouze dvojitou hvězdičku **:

```
**.DEF
  ABC.**
  A*.**
```

ale ne jako

```
A**
```

jinak obdržíte zprávu AMQ7226E: `Název profilu je neplatný.`

Poznámka: Při použití zástupných znaků v systémech AIX and Linux **musíte** uzavřít název profilu do jednoduchých uvozovek.

Priority profilu

Důležitým bodem, který je třeba pochopit při používání generických profilů, je priorita, kterou mají profily při rozhodování o tom, která oprávnění se mají použít na vytvářený objekt. Předpokládejme například, že jste zadali příkazy:

```
setmqaut -n AB.* -t q +put -p fred
setmqaut -n AB.C* -t q +get -p fred
```

První poskytuje oprávnění ke všem frontám pro činitele s názvy, které odpovídají profilu AB. *; druhý poskytuje oprávnění k získání pro stejné typy front, které odpovídají profilu AB.C*.

Předpokládejme, že nyní vytvoříte frontu s názvem AB.CD. Podle pravidel pro porovnávání se zástupnými znaky se na tuto frontu může vztahovat buď setmqaut. Tak, má to dát, nebo získat autoritu?

Chcete-li najít odpověď, použijte pravidlo, které vždy, když lze na objekt použít více profilů, **použije se pouze nejspecifičtější**. Toto pravidlo použijete tak, že porovnáte názvy profilů zleva doprava. Kdekoli se liší, negenerický znak je specifičtější než generický znak. V tomto příkladu tedy jde o frontu AB.CD má oprávnění **získat** (AB.C* je specifičtější než AB. *).

Při porovnávání generických znaků je pořadí *specifičnosti* následující:

1. ?
2. *
3. **

Výpis paměti nastavení profilu

Úplnou definici řídicího příkazu **dmpmqaut** a jeho syntaxi viz dmpmqaut.

Úplnou definici příkazu **DISPLAY AUTHREC** MQSC a jeho syntaxi naleznete v části DISPLAY AUTHREC.

Úplnou definici příkazu **MQCMD_INQUIRE_AUTH_RECS** PCF a jeho syntaxi naleznete v tématu Zdotazovat se na záznamy oprávnění.

Následující příklady ukazují použití řídicího příkazu **dmpmqaut** k výpisu záznamů oprávnění pro generické profily:

1. Tento příklad vypíše všechny záznamy oprávnění s profilem, který odpovídá frontě a.b.c pro činitele user1.

   ```
   dmpmqaut -m qm1 -n a.b.c -t q -p user1
   ```

   Výsledný výpis vypadá přibližně takto:

   ```
   profile:     a.b.*
   object type: queue
   entity:      user1
   type:        principal
   authority:   get, browse, put, inq
   ```

   Poznámka: Ačkoli uživatelé v systému AIX and Linux mohou použít volbu `-p` pro příkaz **dmpmqaut** , musí místo toho při definování autorizací použít `-g groupname` .
2. Tento příklad vypíše všechny záznamy oprávnění s profilem, který odpovídá frontě a.b.c.

   ```
   dmpmqaut -m qmgr1 -n a.b.c -t q
   ```

   Výsledný výpis vypadá přibližně takto:

   ```
   profile:     a.b.c
   object type: queue
   entity:      Administrator
   type:        principal
   authority:   all
   - - - - - - - - - - - - - - - -
   profile:     a.b.*
   object type: queue
   entity:      user1
   type:        principal
   authority:   get, browse, put, inq
   - - - - - - - - - - - - - - - -
   profile:     a.**
   object type: queue
   entity:      group1
   type:        group
   authority:   get
   ```
3. Tento příklad vypíše všechny záznamy oprávnění pro profil a.b. *, typu fronty.

   ```
   dmpmqaut -m qmgr1 -n a.b.* -t q
   ```

   Výsledný výpis vypadá přibližně takto:

   ```
   profile:     a.b.*
   object type: queue
   entity:      user1
   ```

```
type:        principal
authority:   get, browse, put, inq
```

4. Tento příklad vypíše všechny záznamy oprávnění pro správce front qmX.

```
dmpmqaut -m qmX
```

   Výsledný výpis vypadá přibližně takto:

```
profile:     q1
object type: queue
entity:      Administrator
type:        principal
authority:   all
- - - - - - - - - - - - - - - -
profile:     q*
object type: queue
entity:      user1
type:        principal
authority:   get, browse
- - - - - - - - - - - - - - - -
profile:     name.*
object type: namelist
entity:      user2
type:        principal
authority:   get
- - - - - - - - - - - - - - - -
profile:     pr1
object type: process
entity:      group1
type:        group
authority:   get
```

5. Tento příklad vypíše všechny názvy profilů a typy objektů pro správce front qmX.

```
dmpmqaut -m qmX -l
```

   Výsledný výpis vypadá přibližně takto:

```
profile: q1, type: queue
profile: q*, type: queue
profile: name.*, type: namelist
profile: pr1, type: process
```

Poznámka: Pouze pro IBM MQ for Windows všechny zobrazené činitele zahrnují informace o doméně, například:

```
profile:     a.b.*
object type: queue
entity:      user1@domain1
type:        principal
authority:   get, browse, put, inq
```

ALW *Použití zástupných znaků v profilech OAM na systému AIX, Linux, and Windows*

Použijte zástupné znaky v názvu profilu OAM (Object Authority Manager), abyste tento profil učinili použitelným pro více než jeden objekt.

Profil je generický použitím speciálních znaků (zástupných znaků) v názvu profilu. Zástupný znak otazník (?) například odpovídá libovolnému jednotlivému znaku v názvu. Pokud tedy zadáte hodnotu ABC.?EF, bude autorizace, kterou jste udělili tomuto profilu, platit pro všechny objekty s názvy ABC.DEF, ABC.CEF, ABC.BEFatd.

K dispozici jsou následující zástupné znaky:

?

Otazník (?) zastupuje libovolný jeden znak. Například `AB.?D` platí pro objekty `AB.CD`, `AB.EDa AB.FD`.

*****

Použijte hvězdičku (*) jako:

- *Kvalifikátor* v názvu profilu tak, aby odpovídal libovolnému kvalifikátoru v názvu objektu. Kvalifikátor je část názvu objektu oddělená tečkou. Název objektu `ABC.DEF.GHI` se například skládá z kvalifikátorů `ABC`, `DEF` a `GHI`.

  Například `ABC.*.JKL` platí pro objekty `ABC.DEF.JKLa ABC.GHI.JKL`. (Všimněte si, že se **nevztahuje** na `ABC.JKL` ; * použité v tomto kontextu vždy označuje jeden kvalifikátor.)
- Znak v kvalifikátoru v názvu profilu, který odpovídá žádnému nebo více znakům v kvalifikátoru v názvu objektu.

  Například `ABC.DE*.JKL` platí pro objekty `ABC.DE.JKL`, `ABC.DEF.JKLa ABC.DEGH.JKL`.

******

Použijte dvojitou hvězdičku (**) **jednou** v názvu profilu jako:

- Celý název profilu, který má odpovídat všem názvům objektů. Pokud například použijete produkt `-t prcs` k identifikaci procesů a poté použijete ** jako název profilu, změníte oprávnění pro všechny procesy.
- Jako počáteční, střední nebo koncový kvalifikátor v názvu profilu odpovídá žádnému nebo více kvalifikátorům v názvu objektu. Například `**.ABC` identifikuje všechny objekty s konečným kvalifikátorem ABC.

Poznámka: Při použití zástupných znaků v systémech AIX and Linux **musíte** uzavřít název profilu do jednoduchých uvozovek.

ALW *Priority profilu na AIX, Linux, and Windows*

Pro jeden objekt lze použít více než jeden generický profil. V tomto případě platí nejspecifičtější pravidlo.

Důležitým bodem, který je třeba pochopit při používání generických profilů, je priorita, kterou mají profily při rozhodování o tom, která oprávnění se mají použít na vytvářený objekt. Předpokládejme například, že jste zadali příkazy:

```
setmqaut -n AB.* -t q +put -p fred
setmqaut -n AB.C* -t q +get -p fred
```

První poskytuje oprávnění ke všem frontám pro činitele s názvy, které odpovídají profilu AB. *; druhý poskytuje oprávnění k získání pro stejné typy front, které odpovídají profilu AB.C*.

Předpokládejme, že nyní vytvoříte frontu s názvem AB.CD. Podle pravidel pro porovnávání se zástupnými znaky se na tuto frontu může vztahovat buď setmqaut. Tak, má to dát, nebo získat autoritu?

Chcete-li najít odpověď, použijte pravidlo, které vždy, když lze na objekt použít více profilů, **použije se pouze nejspecifičtější**. Toto pravidlo použijete tak, že porovnáte názvy profilů zleva doprava. Kdekoli se liší, negenerický znak je specifičtější než generický znak. V tomto příkladu tedy jde o frontu AB.CD má oprávnění **získat** (AB.C* je specifičtější než AB. *).

Při porovnávání generických znaků je pořadí *specifičnosti* následující:

1. ?
2. *
3. **

Ekvivalentní informace při použití tohoto příkazu MQSC viz SET AUTHREC .

ALW *Výpis nastavení profilu na AIX, Linux, and Windows*

Pomocí řídicího příkazu **dmpmqaut** , příkazu **DISPLAY AUTHREC** MQSC nebo příkazu **MQCMD_INQUIRE_AUTH_RECS** PCF můžete vypsat aktuální autorizace přidružené k určenému profilu. Všimněte si, že v systému IBM MQ Appliance můžete použít pouze příkaz **DISPLAY AUTHREC** .

Úplnou definici řídicího příkazu **dmpmqaut** a jeho syntaxi viz dmpmqaut.

Úplnou definici příkazu **DISPLAY AUTHREC** MQSC a jeho syntaxi naleznete v části DISPLAY AUTHREC.

Úplnou definici příkazu **MQCMD_INQUIRE_AUTH_RECS** PCF a jeho syntaxi naleznete v tématu Zdotazovat se na záznamy oprávnění.

Následující příklady ukazují použití řídicího příkazu **dmpmqaut** k výpisu záznamů oprávnění pro generické profily:

1. Tento příklad vypíše všechny záznamy oprávnění s profilem, který odpovídá frontě a.b.c pro činitele user1.

   ```
   dmpmqaut -m qm1 -n a.b.c -t q -p user1
   ```

   Výsledný výpis vypadá podobně jako v tomto příkladu:

   ```
   profile:     a.b.*
   object type: queue
   entity:      user1
   type:        principal
   authority:   get, browse, put, inq
   ```

   Poznámka: Uživatelé produktu AIX and Linux nemohou použít volbu `-p` ; místo toho musí použít volbu `-g groupname` .
2. Tento příklad vypíše všechny záznamy oprávnění s profilem, který odpovídá frontě a.b.c.

   ```
   dmpmqaut -m qmgr1 -n a.b.c -t q
   ```

   Výsledný výpis vypadá podobně jako v tomto příkladu:

   ```
   profile:     a.b.c
   object type: queue
   entity:      Administrator
   type:        principal
   authority:   all
   - - - - - - - - - - - - - - - -
   profile:     a.b.*
   object type: queue
   entity:      user1
   type:        principal
   authority:   get, browse, put, inq
   - - - - - - - - - - - - - - - -
   profile:     a.**
   object type: queue
   entity:      group1
   type:        group
   authority:   get
   ```
3. Tento příklad vypíše všechny záznamy oprávnění pro profil a.b. *, typu fronty.

   ```
   dmpmqaut -m qmgr1 -n a.b.* -t q
   ```

   Výsledný výpis vypadá podobně jako v tomto příkladu:

   ```
   profile:     a.b.*
   object type: queue
   entity:      user1
   ```

```
type:        principal
authority:   get, browse, put, inq
```

4. Tento příklad vypíše všechny záznamy oprávnění pro správce front qmX.

```
dmpmqaut -m qmX
```

   Výsledný výpis vypadá podobně jako v tomto příkladu:

```
profile:     q1
object type: queue
entity:      Administrator
type:        principal
authority:   all
- - - - - - - - - - - - - - - -
profile:     q*
object type: queue
entity:      user1
type:        principal
authority:   get, browse
- - - - - - - - - - - - - - - -
profile:     name.*
object type: namelist
entity:      user2
type:        principal
authority:   get
- - - - - - - - - - - - - - - -
profile:     pr1
object type: process
entity:      group1
type:        group
authority:   get
```

5. Tento příklad vypíše všechny názvy profilů a typy objektů pro správce front qmX.

```
dmpmqaut -m qmX -l
```

   Výsledný výpis vypadá podobně jako v tomto příkladu:

```
profile: q1, type: queue
profile: q*, type: queue
profile: name.*, type: namelist
profile: pr1, type: process
```

Poznámka: Pouze pro IBM MQ for Windows všechny zobrazené činitele zahrnují informace o doméně, například:

```
profile:     a.b.*
object type: queue
entity:      user1@domain1
type:        principal
authority:   get, browse, put, inq
```

ALW Zobrazení nastavení přístupu na systému AIX, Linux, and Windows

Pomocí řídicího příkazu **dspmqaut** , příkazu **DISPLAY AUTHREC** MQSC nebo příkazu **MQCMD_INQUIRE_ENTITY_AUTH** PCF můžete zobrazit oprávnění, která má konkrétní činitel nebo skupina pro konkrétní objekt. Všimněte si, že v systému IBM MQ Appliance můžete použít pouze příkaz **DISPLAY AUTHREC** .

Chcete-li použít tento příkaz, musí být spuštěn správce front. Když změníte přístup pro činitele, změny se okamžitě projeví v OAM. Autorizaci lze v daném okamžiku zobrazit pouze pro jednu skupinu nebo činitele.

Úplnou definici řídicího příkazu **dmpmqaut** a jeho syntaxi viz dmpmqaut.

Úplnou definici příkazu **DISPLAY AUTHREC** MQSC a jeho syntaxi naleznete v části DISPLAY AUTHREC.

Úplnou definici příkazu **MQCMD_INQUIRE_AUTH_RECS** PCF a jeho syntaxi naleznete v tématu Zdotazovat se na záznamy oprávnění.

Následující příklad ukazuje použití řídicího příkazu **dspmqaut** k zobrazení autorizací, které má skupina GpAdmin k definici procesu s názvem Annuities ve správci front QueueMan1.

```
dspmqaut -m QueueMan1 -t process -n Annuities -g GpAdmin
```

ALW Změna a zrušení přístupu k objektu IBM MQ v systému AIX, Linux, and Windows

Chcete-li změnit úroveň přístupu uživatele nebo skupiny k objektu, použijte řídicí příkaz **setmqaut** , příkaz **DELETE AUTHREC** MQSC nebo příkaz **MQCMD_DELETE_AUTH_REC** PCF. MQ Appliance Všimněte si, že na serveru IBM MQ Appliance můžete použít pouze příkaz **DELETE AUTHREC** .

Proces odebrání uživatele ze skupiny je popsán v:

- Windows "Vytvoření a správa skupin v systému Windows" na stránce 147
- AIX "Vytvoření a správa skupin v systému AIX" na stránce 146
- Linux "Vytvoření a správa skupin v systému Linux" na stránce 147

.

ID uživatele, který vytváří objekt IBM MQ , má k tomuto objektu udělena úplná oprávnění k řízení. Pokud toto ID uživatele odeberete z lokální skupiny mqm (nebo ze skupiny Administrators v systémech Windows), nebudou tato oprávnění odvolána. Pomocí řídicího příkazu **setmqaut** nebo příkazu **MQCMD_DELETE_AUTH_REC** PCF můžete zrušit přístup k objektu pro ID uživatele, který jej vytvořil, po jeho odebrání ze skupiny administrátorů nebo mqm.

Úplnou definici řídicího příkazu setmqaut a jeho syntaxi naleznete v tématu setmqaut.

Úplnou definici příkazu **DELETE AUTHREC** MQSC a jeho syntaxi naleznete v tématu DELETE AUTHREC.

Úplnou definici příkazu **MQCMD_DELETE_AUTH_REC** PCF a jeho syntaxi naleznete v tématu Odstranění záznamu oprávnění.

Windows V systému Windowsmůžete z adresáře IBM MQ 8.0kdykoli odstranit položky OAM odpovídající konkrétnímu uživatelskému účtu Windows pomocí parametru **-u** *SID* **setmqaut**.

Před IBM MQ 8.0jste museli odstranit položky OAM odpovídající konkrétnímu uživatelskému účtu Windows před odstraněním uživatelského profilu. Po odebrání uživatelského účtu nebylo možné odebrat položky OAM.

ALW Zabránění kontrolám zabezpečených přístupů na systémech AIX, Linux, and Windows

Poznámka: Toto téma popisuje funkčnost, která se nedoporučuje povolit. Chcete-li vypnout kontrolu zabezpečení, můžete zakázat správce oprávnění k objektu (OAM). To může být vhodné pro testovací prostředí. Je-li tato volba zakázána, správce front již nebude moci provádět kontroly ověření autorizace nebo připojení. Nadále lze používat protokoly TLS, záznamy ověřování kanálu a uživatelské procedury zabezpečení. Po zakázání nebo odebrání modulu OAM nelze přidat modul OAM do existujícího správce front.

Pokud se rozhodnete, že nechcete provádět kontroly zabezpečení (například v testovacím prostředí), můžete OAM zakázat jedním ze dvou způsobů:

- Před vytvořením správce front nastavte proměnnou prostředí operačního systému **MQSNOAUT**.

  Informace o důsledcích nastavení proměnné prostředí **MQSNOAUT** a způsobu nastavení **MQSNOAUT** na AIX, Linux, and Windowsviz Popisy proměnných prostředí.

- Upravte konfigurační soubor správce front a odeberte službu.

Upozornění: Je-li modul OAM odebrán, nelze jej vrátit zpět do existujícího správce front. Je to proto, že OAM musí být na místě v době vytvoření objektu. Chcete-li znovu použít modul OAM IBM MQ po jeho odebrání, znovu sestavte správce front.

Pokud používáte příkaz **setmqaut**nebo **dspmqaut** , když je OAM vypnutý, poznamenejte si následující body:

- OAM neověřuje uvedeného činitele nebo skupinu, což znamená, že příkaz může přijmout neplatné hodnoty.
- OAM neprovádí kontroly zabezpečení a označuje, že všichni činitelé a skupiny jsou autorizováni k provedení všech použitelných operací s objekty.
- Žádná pověření předaná OAM pro kontroly ověření nejsou ověřena.

Související pojmy

Instalovatelné služby a komponenty pro AIX, Linux, and Windows

Související úlohy

Konfigurace instalovatelných služeb

Související odkazy

Referenční informace o instalovatelných službách

Udělení požadovaného přístupu k prostředkům

Toto téma slouží k určení úloh, které mají být provedeny pro použití zabezpečení v systému IBM MQ .

Informace o této úloze

Během této úlohy se rozhodnete, jaké akce jsou nezbytné pro použití odpovídající úrovně zabezpečení na prvky vaší instalace produktu IBM MQ . Každý jednotlivý úkol, na který se odkazujete, poskytuje podrobné pokyny pro všechny platformy.

Postup

1. Potřebujete omezit přístup ke správci front na určité uživatele?
   a) Ne: Neprovádějte žádné další kroky.
   b) Ano: Jděte na další otázku.
2. Potřebují tito uživatelé částečný administrativní přístup k podmnožině prostředků správce front?
   a) Ne: Jděte na další otázku.
   b) Ano: Viz “Udělení částečného administrativního přístupu k podmnožině prostředků správce front” na stránce 384.
3. Potřebují tito uživatelé úplný administrativní přístup k podmnožině prostředků správce front?
   a) Ne: Jděte na další otázku.
   b) Ano: Viz “Udělení úplného administrativního přístupu k podmnožině prostředků správce front” na stránce 392.
4. Potřebují tito uživatelé přístup jen pro čtení ke všem prostředkům správce front?
   a) Ne: Jděte na další otázku.
   b) Ano: Viz “Udělení přístupu jen pro čtení ke všem prostředkům ve správci front” na stránce 398.
5. Potřebují tito uživatelé úplný administrativní přístup ke všem prostředkům správce front?
   a) Ne: Jděte na další otázku.
   b) Ano: Viz “Udělení úplného administrativního přístupu ke všem prostředkům ve správci front” na stránce 400.
6. Potřebujete uživatelské aplikace pro připojení ke správci front?

a) Ne: Zakázat konektivitu, jak je popsáno v tématu “Odebrání konektivity ke správci front” na stránce 401

b) Ano: Viz “Povolení připojení uživatelských aplikací ke správci front” na stránce 402.

Multi z/OS Udělení částečného administrativního přístupu k podmnožině prostředků správce front

Určitým uživatelům musíte poskytnout částečný administrativní přístup k některým, ale ne všem prostředkům správce front. Tuto tabulku použijte k určení akcí, které musíte provést.

Tabulka 72. Udělení částečného administrativního přístupu k podmnožině prostředků správce front

Uživatelé musí spravovat objekty tohoto typu	**Provést tuto akci**
Fronty	Udělte částečný administrativní přístup k požadovaným frontám, jak je popsáno v tématu “Udělení omezeného administrativního přístupu k některým frontám” na stránce 384 .
Témata	Udělte částečný administrativní přístup k požadovaným tématům, jak je popsáno v tématu “Udělení omezeného administrativního přístupu k některým tématům” na stránce 386 .
Kanály	Udělte částečný administrativní přístup k požadovaným kanálům, jak je popsáno v tématu “Udělení omezeného administrativního přístupu k některým kanálům” na stránce 387 .
Správce front	Udělte správci front částečný administrativní přístup, jak je popsáno v tématu “Udělení omezeného administrativního přístupu ke správci front” na stránce 388 .
Procesy	Udělte částečný administrativní přístup k požadovaným procesům, jak je popsáno v tématu “Udělení omezeného administrativního přístupu k některým procesům” na stránce 389 .
Seznamy názvů	Udělte částečný administrativní přístup k požadovaným seznamům názvů, jak je popsáno v tématu “Udělení omezeného administrativního přístupu k některým seznamům názvů” na stránce 390 .
Služby	Udělte částečný administrativní přístup k požadovaným službám, jak je popsáno v tématu “Udělení omezeného administrativního přístupu k některým službám” na stránce 391 .

Udělení omezeného administrativního přístupu k některým frontám

Udělte částečný administrativní přístup k některým frontám ve správci front každé skupině uživatelů s obchodní potřebou.

Informace o této úloze

Chcete-li udělit omezený administrativní přístup k některým frontám pro některé akce, použijte odpovídající příkazy pro váš operační systém.

Na platformách Multiplatforms můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Procedura

- ALW
  Pro systémy AIX, Linux, and Windows zadejte následující příkaz:

  ```
  setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName ReqdAction
  ```

- IBM i
  Pro systém IBM izadejte následující příkaz:

  ```
  GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(ReqdAction) MQMNAME('
  QMgrName ')
  ```

- z/OS Pro systém z/OSzadejte následující příkazy pro udělení přístupu k uvedené frontě:

  ```
  RDEFINE MQADMIN QMgrName.QUEUE. ObjectProfile UACC(NONE)
  PERMIT QMgrName.QUEUE. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
  ```

  Chcete-li určit, které příkazy MQSC může uživatel ve frontě provádět, zadejte pro každý příkaz MQSC následující příkazy:

  ```
  RDEFINE MQCMDS QMgrName. ReqdAction. QType UACC(NONE)
  PERMIT QMgrName. ReqdAction. QType CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
  ```

  Chcete-li uživateli povolit použití příkazu DISPLAY QUEUE, zadejte následující příkazy:

  ```
  RDEFINE MQCMDS QMgrName.DISPLAY. QType UACC(NONE)
  PERMIT QMgrName.DISPLAY. QType CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
  ```

  Názvy proměnných mají následující význam:

  QMgrName
  Název správce front.

  z/OS V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.

  ObjectProfile
  Název objektu nebo generického profilu, pro který se mají změnit autorizace.

  GroupName
  Název skupiny, které má být udělen přístup.

  ReqdAction
  Akce, kterou povolujete skupině provést:

  – ALW V systémech AIX, Linux, and Windows se jedná o libovolnou kombinaci následujících oprávnění: + chg, + clr, + dlt, + dsp. Oprávnění + alladm je ekvivalentní + chg + clr + dlt + dsp.

  – IBM i V systému IBM i, libovolná kombinace následujících oprávnění: *ADMCHG, *ADMCLR, *ADMDLT, *ADMDSP. Oprávnění *ALLADM je ekvivalentní všem těmto individuálním autorizacím.

  – z/OS V systému z/OSse jedná o jednu z hodnot ALTER, CLEAR, DELETE nebo MOVE.

  Poznámka: Udělení + crt pro fronty nepřímo učiní uživatele nebo skupinu administrátorem. K udělení omezeného administrativního přístupu k některým frontám nepoužívejte oprávnění + crt.

QTYPE

Pro příkaz DISPLAY je to jedna z hodnot QUEUE, QLOCAL, QALIAS, QMODEL, QREMOTE nebo QCLUSTER.

Pro ostatní hodnoty *ReqdAction*jedna z hodnot QLOCAL, QALIAS, QMODEL nebo QREMOTE.

Udělení omezeného administrativního přístupu k některým tématům

Udělte částečný administrativní přístup k některým tématům ve správci front pro každou skupinu uživatelů s obchodní potřebou.

Informace o této úloze

Chcete-li udělit omezený administrativní přístup k některým tématům pro některé akce, použijte příslušné příkazy pro váš operační systém.

Na platformách Multiplatforms můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Procedura

- ALW

  Pro systémy AIX, Linux, and Windows zadejte následující příkaz:

  ```
  setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName ReqdAction
  ```

- IBM i

  Pro systém IBM izadejte následující příkaz:

  ```
  GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*TOPIC) USER(GroupName) AUT(ReqdAction) MQMNAME('
  QMgrName ')
  ```

- z/OS Pro systém z/OSzadejte následující příkazy:

  ```
  RDEFINE MQADMIN QMgrName.TOPIC. ObjectProfile UACC(NONE)
  PERMIT QMgrName.TOPIC. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
  ```

  Tyto příkazy udělují přístup k zadanému tématu. Chcete-li určit, které příkazy MQSC může uživatel s daným tématem provádět, zadejte pro každý příkaz MQSC následující příkazy:

  ```
  RDEFINE MQCMDS QMgrName. ReqdAction.TOPIC UACC(NONE)
  PERMIT QMgrName. ReqdAction.TOPIC CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
  ```

  Chcete-li uživateli povolit použití příkazu DISPLAY TOPIC, zadejte následující příkazy:

  ```
  RDEFINE MQCMDS QMgrName.DISPLAY.TOPIC UACC(NONE)
  PERMIT QMgrName.DISPLAY.TOPIC CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
  ```

  Názvy proměnných mají následující význam:

  QMgrName
  Název správce front.

  z/OS V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.

  ObjectProfile
  Název objektu nebo generického profilu, pro který se mají změnit autorizace.

GroupName
Název skupiny, které má být udělen přístup.

ReqdAction
Akce, kterou povolujete skupině provést:

- ALW V systémech AIX, Linux, and Windows se jedná o libovolnou kombinaci následujících oprávnění: + chg, + clr, + crt, + dlt, + dsp. + trsátko. Oprávnění + alladm je ekvivalentní + chg + clr + dlt + dsp.
- IBM i V systému IBM i, libovolná kombinace následujících oprávnění: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP, *CTRL. Oprávnění *ALLADM je ekvivalentní všem těmto individuálním autorizacím.
- z/OS V systému z/OSse jedná o jednu z hodnot ALTER, CLEAR, DEFINE, DELETE nebo MOVE.

Udělení omezeného administrativního přístupu k některým kanálům

Udělte částečný administrativní přístup k některým kanálům ve správci front každé skupině uživatelů s obchodní potřebou.

Informace o této úloze

Chcete-li některým akcím udělit omezený administrativní přístup k některým kanálům, použijte příslušné příkazy pro váš operační systém.

Na platformách Multiplatforms můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Procedura

- ALW
  V systému AIX, Linux, and Windows:

```
setmqaut -m QMgrName -n ObjectProfile -t channel -g GroupName ReqdAction
```

- IBM i
  V systému IBM i:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*CHL) USER(GroupName) AUT(ReqdAction) MQMNAME('
QMgrName ')
```

- z/OS V systému z/OS:

```
RDEFINE MQADMIN QMgrName.CHANNEL. ObjectProfile UACC(NONE)
PERMIT QMgrName.CHANNEL. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

  Tyto příkazy udělují přístup k určenému kanálu. Chcete-li určit, které příkazy MQSC může uživatel v kanálu provádět, zadejte pro každý příkaz MQSC následující příkazy:

```
RDEFINE MQCMDS QMgrName. ReqdAction.CHANNEL UACC(NONE)
PERMIT QMgrName. ReqdAction.CHANNEL CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
```

  Chcete-li uživateli povolit použití příkazu DISPLAY CHANNEL, zadejte následující příkazy:

```
RDEFINE MQCMDS QMgrName.DISPLAY.CHANNEL UACC(NONE)
PERMIT QMgrName.DISPLAY.CHANNEL CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

Názvy proměnných mají následující význam:

QMgrName
Název správce front.

z/OS V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.

ObjectProfile
Název objektu nebo generického profilu, pro který se mají změnit autorizace.

GroupName
Název skupiny, které má být udělen přístup.

ReqdAction
Akce, kterou povolujete skupině provést:

- ALW V systému AIX, Linux, and Windowsse jedná o libovolnou kombinaci následujících oprávnění: + chg, + clr, + crt, + dlt, + dsp. + ctrl, + ctrlx. Oprávnění + alladm je ekvivalentní + chg + clr + dlt + dsp.
- IBM i V systému IBM i, libovolná kombinace následujících oprávnění: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP, *CTRL, *CTRLx. Oprávnění *ALLADM je ekvivalentní všem těmto individuálním autorizacím.
- z/OS V systému z/OSse jedná o jednu z hodnot ALTER, CLEAR, DEFINE, DELETE nebo MOVE.

Udělení omezeného administrativního přístupu ke správci front

Udělte částečný administrativní přístup ke správci front každé skupině uživatelů s obchodní potřebou.

Informace o této úloze

Chcete-li udělit omezený administrativní přístup k provádění některých akcí ve správci front, použijte příslušné příkazy pro váš operační systém.

Na platformách Multiplatforms můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Procedura

- ALW
  V systému AIX, Linux, and Windows:

```
setmqaut -m QMgrName -n ObjectProfile -t qmgr -g GroupName ReqdAction
```

- IBM i
  V systému IBM i:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*MQM) USER(GroupName) AUT(ReqdAction) MQMNAME('
QMgrName ')
```

- z/OS
  V systému z/OS:

  Chcete-li zjistit, které příkazy MQSC můžete ve správci front provádět, zadejte pro každý příkaz MQSC následující příkazy:

```
RDEFINE MQCMDS QMgrName. ReqdAction.QMGR UACC(NONE)
PERMIT QMgrName. ReqdAction.QMGR CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
```

Chcete-li uživateli povolit použití příkazu DISPLAY QMGR, zadejte následující příkazy:

```
RDEFINE MQCMDS QMgrName.DISPLAY.QMGR UACC(NONE)
PERMIT QMgrName.DISPLAY.QMGR CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

Názvy proměnných mají následující význam:

QMgrName
Název správce front.

ObjectProfile
Název objektu nebo generického profilu, pro který se mají změnit autorizace.

GroupName
Název skupiny, které má být udělen přístup.

ReqdAction
Akce, kterou povolujete skupině provést:

- ALW V systému AIX, Linux, and Windowsse jedná o libovolnou kombinaci následujících oprávnění: + chg, + clr, + crt, + dlt, + dsp. Oprávnění + alladm je ekvivalentní + chg + clr + dlt + dsp.

  Ačkoli + set je autorizace MQI a není obvykle považována za administrativní, udělení + sady ve správci front může nepřímo vést k úplnému administrativnímu oprávnění. Neudělujte + sadu běžným uživatelům a aplikacím.
- IBM i V systému IBM i, libovolná kombinace následujících oprávnění: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP. Oprávnění *ALLADM je ekvivalentní všem těmto individuálním autorizacím.

Udělení omezeného administrativního přístupu k některým procesům

Udělte částečný administrativní přístup k některým procesům ve správci front každé skupině uživatelů s obchodní potřebou.

Informace o této úloze

Chcete-li některým akcím udělit omezený administrativní přístup k některým procesům, použijte příslušné příkazy pro váš operační systém.

Na platformách Multiplatforms můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Procedura

- ALW
  V systému AIX, Linux, and Windows:

  ```
  setmqaut -m QMgrName -n ObjectProfile -t process -g GroupName ReqdAction
  ```
- IBM i
  V systému IBM i:

  ```
  GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*PRC) USER(GroupName) AUT(ReqdAction) MQMNAME('
  QMgrName ')
  ```
- z/OS V systému z/OS:

```
RDEFINE MQADMIN QMgrName.PROCESS. ObjectProfile UACC(NONE)
PERMIT QMgrName.PROCESS. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

Tyto příkazy udělují přístup k určenému kanálu. Chcete-li určit, které příkazy MQSC může uživatel v kanálu provádět, zadejte pro každý příkaz MQSC následující příkazy:

```
RDEFINE MQCMDS QMgrName. ReqdAction.PROCESS UACC(NONE)
PERMIT QMgrName. ReqdAction.PROCESS CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
```

Chcete-li uživateli povolit použití příkazu DISPLAY PROCESS, zadejte následující příkazy:

```
RDEFINE MQCMDS QMgrName.DISPLAY.PROCESS UACC(NONE)
PERMIT QMgrName.DISPLAY.PROCESS CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

Názvy proměnných mají následující význam:

QMgrName
Název správce front.

z/OS V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.

ObjectProfile
Název objektu nebo generického profilu, pro který se mají změnit autorizace.

GroupName
Název skupiny, které má být udělen přístup.

ReqdAction
Akce, kterou povolujete skupině provést:

- ALW V systému AIX, Linux, and Windowsse jedná o libovolnou kombinaci následujících oprávnění: + chg, + clr, + crt, + dlt, + dsp. Oprávnění + alladm je ekvivalentní + chg + clr + dlt + dsp.
- IBM i V systému IBM i, libovolná kombinace následujících oprávnění: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP. Oprávnění *ALLADM je ekvivalentní všem těmto individuálním autorizacím.
- z/OS V systému z/OSse jedná o jednu z hodnot ALTER, CLEAR, DEFINE, DELETE nebo MOVE.

Udělení omezeného administrativního přístupu k některým seznamům názvů

Udělte částečný administrativní přístup k některým seznamům názvů ve správci front pro každou skupinu uživatelů s obchodní potřebou.

Informace o této úloze

Chcete-li některým akcím udělit omezený administrativní přístup k některým seznamům názvů, použijte příslušné příkazy pro váš operační systém.

Na platformách Multiplatforms můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Procedura

- ALW
  V systému AIX, Linux, and Windows:

```
setmqaut -m QMgrName -n ObjectProfile -t namelist -g GroupName ReqdAction
```

- IBM i
  V systému IBM i:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*NMLIST) USER(GroupName) AUT(ReqdAction) MQMNAME('
QMgrName ')
```

- z/OS V systému z/OS:

```
RDEFINE MQADMIN QMgrName.NAMELIST. ObjectProfile UACC(NONE)
PERMIT QMgrName.NAMELIST. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

  Tyto příkazy udělují přístup k zadanému seznamu názvů. Chcete-li zjistit, které příkazy MQSC může uživatel v seznamu názvů provádět, zadejte pro každý příkaz MQSC následující příkazy:

```
RDEFINE MQCMDS QMgrName. ReqdAction.NAMELIST UACC(NONE)
PERMIT QMgrName. ReqdAction.NAMELIST CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
```

  Chcete-li uživateli povolit použití příkazu DISPLAY NAMELIST, zadejte následující příkazy:

```
RDEFINE MQCMDS QMgrName.DISPLAY.NAMELIST UACC(NONE)
PERMIT QMgrName.DISPLAY.NAMELIST CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

  Názvy proměnných mají následující význam:

  QMgrName
  Název správce front.

  z/OS V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.

  ObjectProfile
  Název objektu nebo generického profilu, pro který se mají změnit autorizace.

  GroupName
  Název skupiny, které má být udělen přístup.

  ReqdAction
  Akce, kterou povolujete skupině provést:

  - ALW V systému AIX, Linux, and Windowsse jedná o libovolnou kombinaci následujících oprávnění: + chg, + clr, + crt, + dlt, + ctrl, + ctrlx, + dsp. Oprávnění + alladm je ekvivalentní + chg + clr + dlt + dsp.
  - IBM i V systému IBM ise jedná o libovolnou kombinaci následujících oprávnění: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP, *CTRL, *CTRLX. Oprávnění *ALLADM je ekvivalentní všem těmto individuálním autorizacím.
  - z/OS V systému z/OSse jedná o jednu z hodnot ALTER, CLEAR, DEFINE, DELETE nebo MOVE.

Udělení omezeného administrativního přístupu k některým službám

Udělte částečný administrativní přístup k některým službám ve správci front každé skupině uživatelů s obchodní potřebou.

Informace o této úloze

Chcete-li udělit omezený administrativní přístup k některým službám pro některé akce, použijte příslušné příkazy pro váš operační systém. z/OS Všimněte si, že objekty služeb v systému z/OSneexistují.

Na platformách Multiplatforms můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Procedura

- ALW
  V systému AIX, Linux, and Windows:

```
setmqaut -m QMgrName -n ObjectProfile -t service -g GroupName ReqdAction
```

- V systému IBM i:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*SVC) USER(GroupName) AUT(ReqdAction) MQMNAME('
QMgrName ')
```

- z/OS V systému z/OS:

  Tyto příkazy udělují přístup k uvedené službě. Chcete-li určit, které příkazy MQSC může uživatel ve službě provádět, zadejte pro každý příkaz MQSC následující příkazy:

```
RDEFINE MQCMDS QMgrName. ReqdAction.SERVICE UACC(NONE)
PERMIT QMgrName. ReqdAction.SERVICE CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
```

  Chcete-li uživateli povolit použití příkazu DISPLAY SERVICE, zadejte následující příkazy:

```
RDEFINE MQCMDS QMgrName.DISPLAY.SERVICE UACC(NONE)
PERMIT QMgrName.DISPLAY.SERVICE CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

  Názvy proměnných mají následující význam:

  QMgrName
  Název správce front.

  ObjectProfile
  Název objektu nebo generického profilu, pro který se mají změnit autorizace.

  GroupName
  Název skupiny, které má být udělen přístup.

  ReqdAction
  Akce, kterou povolujete skupině provést:

  – ALW V systémech AIX, Linux, and Windows se jedná o libovolnou kombinaci následujících oprávnění: + chg, + clr, + crt, + dlt, + ctrl, + ctrlx, + dsp. Oprávnění + alladm je ekvivalentní + chg + clr + dlt + dsp.

  – IBM i V systému IBM ise jedná o libovolnou kombinaci následujících oprávnění: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP, *CTRL, *CTRLX. Oprávnění *ALLADM je ekvivalentní všem těmto individuálním autorizacím.

Udělení úplného administrativního přístupu k podmnožině prostředků správce front

Určitým uživatelům musíte poskytnout úplný administrativní přístup k některým, ale ne ke všem prostředkům správce front. Pomocí těchto tabulek určete akce, které je třeba provést.

Tabulka 73. Udělení úplného administrativního přístupu k podmnožině prostředků správce front

Uživatelé musí spravovat objekty tohoto typu	**Provést tuto akci**
Fronty	Udělte úplný administrativní přístup k požadovaným frontám, jak je popsáno v tématu “Udělení úplného administrativního přístupu k některým frontám” na stránce 393 .

Tabulka 73. Udělení úplného administrativního přístupu k podmnožině prostředků správce front (pokračování)	
Uživatelé musí spravovat objekty tohoto typu	**Provést tuto akci**
Témata	Udělte úplný administrativní přístup k požadovaným tématům, jak je popsáno v tématu “Udělení úplného administrativního přístupu k některým tématům” na stránce 394 .
Kanály	Udělte úplný administrativní přístup k požadovaným kanálům, jak je popsáno v tématu “Udělení úplného administrativního přístupu k některým kanálům” na stránce 395 .
Správce front	Udělte úplný administrativní přístup ke správci front, jak je popsáno v tématu “Udělení úplného administrativního přístupu ke správci front” na stránce 395 .
Procesy	Udělte úplný administrativní přístup k požadovaným procesům, jak je popsáno v tématu “Udělení úplného administrativního přístupu k některým procesům” na stránce 396 .
Seznamy názvů	Udělte úplný administrativní přístup k požadovaným seznamům názvů, jak je popsáno v tématu “Udělení úplného administrativního přístupu k některým seznamům názvů” na stránce 397 .
Služby	Udělte úplný administrativní přístup k požadovaným službám, jak je popsáno v tématu “Udělení úplného administrativního přístupu k některým službám” na stránce 398 .

Udělení úplného administrativního přístupu k některým frontám

Udělte úplný administrativní přístup k některým frontám ve správci front každé skupině uživatelů s obchodní potřebou.

Informace o této úloze

Chcete-li udělit úplný administrativní přístup k některým frontám, použijte odpovídající příkazy pro váš operační systém.

Na platformách Multiplatforms můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Procedura

- ALW
  V systému AIX, Linux, and Windows:

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +alladm
```

- IBM i
  V systému IBM i:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*ALLADM) MQMNAME(' QMgrName
')
```

- z/OS

  V systému z/OS:

```
RDEFINE MQADMIN QMgrName.QUEUE. ObjectProfile UACC(NONE)
PERMIT QMgrName.QUEUE. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

  Názvy proměnných mají následující význam:

  QMgrName
  Název správce front.

  z/OS V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.

  ObjectProfile
  Název objektu nebo generického profilu, pro který se mají změnit autorizace.

  GroupName
  Název skupiny, které má být udělen přístup.

Udělení úplného administrativního přístupu k některým tématům

Udělte úplný administrativní přístup k některým tématům ve správci front každé skupině uživatelů s obchodní potřebou.

Informace o této úloze

Chcete-li udělit úplný administrativní přístup k některým tématům pro některé akce, použijte příslušné příkazy pro váš operační systém.

Na platformách Multiplatforms můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Procedura

- ALW

  V systému AIX, Linux, and Windows:

```
setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName +alladm
```

- IBM i

  V systému IBM i:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*TOPIC) USER(GroupName) AUT(ALLADM) MQMNAME('
QMgrName ')
```

- z/OS

  V systému z/OS:

```
RDEFINE MQADMIN QMgrName.TOPIC. ObjectProfile UACC(NONE)
PERMIT QMgrName.TOPIC. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

  Názvy proměnných mají následující význam:

  QMgrName
  Název správce front.

z/OS V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.

ObjectProfile
Název objektu nebo generického profilu, pro který se mají změnit autorizace.

GroupName
Název skupiny, které má být udělen přístup.

Udělení úplného administrativního přístupu k některým kanálům

Udělte úplný administrativní přístup k některým kanálům ve správci front každé skupině uživatelů s obchodní potřebou.

Informace o této úloze

Chcete-li udělit úplný administrativní přístup k některým kanálům, použijte odpovídající příkazy pro váš operační systém.

Na platformách Multiplatforms můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Procedura

- ALW
  V systému AIX, Linux, and Windows:

```
setmqaut -m QMgrName -n ObjectProfile -t channel -g GroupName +alladm
```

- IBM i
  V systému IBM i:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*CHL) USER(GroupName) AUT(ALLADM) MQMNAME('
QMgrName ')
```

- z/OS
  V systému z/OS:

```
RDEFINE MQADMIN QMgrName.CHANNEL. ObjectProfile UACC(NONE)
PERMIT QMgrName.CHANNEL. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

  Názvy proměnných mají následující význam:

  QMgrName
  Název správce front.

  z/OS V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.

  ObjectProfile
  Název objektu nebo generického profilu, pro který se mají změnit autorizace.

  GroupName
  Název skupiny, které má být udělen přístup.

Udělení úplného administrativního přístupu ke správci front

Udělte úplný administrativní přístup ke správci front pro každou skupinu uživatelů s obchodní potřebou.

Informace o této úloze

Chcete-li udělit úplný administrativní přístup ke správci front, použijte příslušné příkazy pro váš operační systém.

Na platformách Multiplatforms můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Procedura

- ALW
  V systému AIX, Linux, and Windows:

```
setmqaut -m QMgrName -t qmgr -g GroupName +alladm
```

- IBM i
  V systému IBM i:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*MQM) USER(GroupName) AUT(*ALLADM) MQMNAME('
QMgrName ')
```

- z/OS
  V systému z/OS:

```
RDEFINE MQADMIN QMgrName.QMGR UACC(NONE)
PERMIT QMgrName.QMGR CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

  Názvy proměnných mají následující význam:

  QMgrName
  Název správce front.

  z/OS V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.

  ObjectProfile
  Název objektu nebo generického profilu, pro který se mají změnit autorizace.

  GroupName
  Název skupiny, které má být udělen přístup.

Udělení úplného administrativního přístupu k některým procesům

Udělte úplný administrativní přístup k některým procesům ve správci front každé skupině uživatelů s obchodní potřebou.

Informace o této úloze

Chcete-li udělit úplný administrativní přístup k některým procesům, použijte odpovídající příkazy pro váš operační systém.

Na platformách Multiplatforms můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Procedura

- ALW
  V systému AIX, Linux, and Windows:

```
setmqaut -m QMgrName -n ObjectProfile -t process -g GroupName +alladm
```

- IBM i
  V systému IBM i:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*PRC) USER(GroupName) AUT(*ALLADM) MQMNAME('
QMgrName ')
```

- z/OS

  V systému z/OS:

```
RDEFINE MQADMIN QMgrName.CHANNEL. ObjectProfile UACC(NONE)
PERMIT QMgrName.PROCESS. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

  Názvy proměnných mají následující význam:

  QMgrName
  Název správce front.

  z/OS V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.

  ObjectProfile
  Název objektu nebo generického profilu, pro který se mají změnit autorizace.

  GroupName
  Název skupiny, které má být udělen přístup.

Udělení úplného administrativního přístupu k některým seznamům názvů

Udělte úplný administrativní přístup k některým seznamům názvů ve správci front pro každou skupinu uživatelů s obchodní potřebou.

Informace o této úloze

Chcete-li udělit úplný administrativní přístup k některým seznamům názvů, použijte příslušné příkazy pro váš operační systém.

Na platformách Multiplatforms můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Procedura

- ALW

  V systému AIX, Linux, and Windows:

```
setmqaut -m QMgrName -n ObjectProfile -t namelist -g GroupName +alladm
```

- IBM i

  V systému IBM i:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*NMLIST) USER(GroupName) AUT(*ALLADM) MQMNAME('
QMgrName ')
```

- z/OS

  V systému z/OS:

```
RDEFINE MQADMIN QMgrName.NAMELIST. ObjectProfile UACC(NONE)
PERMIT QMgrName.NAMELIST. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

  Názvy proměnných mají následující význam:

  QMgrName
  Název správce front.

z/OS V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.

ObjectProfile
Název objektu nebo generického profilu, pro který se mají změnit autorizace.

GroupName
Název skupiny, které má být udělen přístup.

Udělení úplného administrativního přístupu k některým službám

Udělte úplný administrativní přístup k některým službám ve správci front pro každou skupinu uživatelů s obchodní potřebou.

Informace o této úloze

Chcete-li udělit úplný administrativní přístup k některým službám, použijte odpovídající příkazy pro váš operační systém.

Na platformách Multiplatforms můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Procedura

- ALW
  V systému AIX, Linux, and Windows:

```
setmqaut -m QMgrName -n ObjectProfile -t service -g GroupName +alladm
```

- IBM i
  V systému IBM i:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*SVC) USER(GroupName) AUT(*ALLADM) MQMNAME('
QMgrName ')
```

- z/OS
  V systému z/OS:

```
RDEFINE MQADMIN QMgrName.SERVICE. ObjectProfile UACC(NONE)
PERMIT QMgrName.SERVICE. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

  Názvy proměnných mají následující význam:

  QMgrName
  Název správce front.

  z/OS V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.

  ObjectProfile
  Název objektu nebo generického profilu, pro který se mají změnit autorizace.

  GroupName
  Název skupiny, které má být udělen přístup.

Udělení přístupu jen pro čtení ke všem prostředkům ve správci front

Udělte přístup jen pro čtení ke všem prostředkům ve správci front každému uživateli nebo skupině uživatelů s obchodní potřebou.

Informace o této úloze

Použijte průvodce Přidat oprávnění založená na rolích nebo odpovídající příkazy pro váš operační systém.

Na platformách Multiplatforms můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Po změně podrobností o autorizaci proveďte aktualizaci zabezpečení pomocí příkazu REFRESH SECURITY .

Procedura

- Pomocí průvodce:
  a) V podokně IBM MQ Explorer Navigator klepněte pravým tlačítkem myši na správce front a klepněte na volbu **Oprávnění k objektům** > **Přidat oprávnění založená na rolích**

  Otevře se průvodce Přidat oprávnění založená na rolích.
- ALW
  V systémech AIX, Linux, and Windows zadejte následující příkazy:

```
setmqaut -m QMgrName -n ** -t queue -g GroupName +browse +dsp
setmqaut -m QMgrName -n SYSTEM.ADMIN.COMMAND.QUEUE -t queue -g GroupName +dsp +inq +put
setmqaut -m QMgrName -n SYSTEM.MQEXPLORER.REPLY.MODEL -t queue -g GroupName +dsp +inq +get
+put
setmqaut -m QMgrName -n ** -t topic -g GroupName +dsp
setmqaut -m QMgrName -n ** -t channel -g GroupName +dsp
setmqaut -m QMgrName -n ** -t clntconn -g GroupName +dsp
setmqaut -m QMgrName -n ** -t authinfo -g GroupName +dsp
setmqaut -m QMgrName -n ** -t listener -g GroupName +dsp
setmqaut -m QMgrName -n ** -t namelist -g GroupName +dsp
setmqaut -m QMgrName -n ** -t process -g GroupName +dsp
setmqaut -m QMgrName -n ** -t service -g GroupName +dsp
setmqaut -m QMgrName -t qmgr -g GroupName +dsp +inq +connect
```

  Specifická oprávnění pro SYSTEM.ADMIN.COMMAND.QUEUE a SYSTEM.MQEXPLORER.REPLY.MODEL je nezbytný pouze v případě, že chcete použít IBM MQ Explorer.
- IBM i
  Pro systém IBM izadejte následující příkazy:

```
GRTMQMAUT OBJ(*ALL) OBJTYPE(*Q) USER('GroupName') AUT(*ADMDSP *BROWSE) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*TOPIC) USER('GroupName') AUT(*ADMDSP) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*CHL) USER('GroupName') AUT(*ADMDSP *INQ) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*CLTCN) USER('GroupName') AUT(*ADMDSP) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*AUTHINFO) USER('GroupName') AUT(*ADMDSP) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*LSR) USER('GroupName') AUT(*ADMDSP)MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*NMLIST) USER('GroupName') AUT(*ADMDSP) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*PRC) USER('GroupName') AUT(*ADMDSP) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*SVC) USER('GroupName') AUT(*ADMDSP) MQMNAME('QMgrName')
GRTMQMAUT OBJ('object-name') OBJTYPE(*MQM) USER('GroupName') AUT(*ADMDSP *CONNECT *INQ)
MQMNAME('QMgrName')
```

- z/OS
  Pro systém z/OSzadejte následující příkazy:

```
RDEFINE MQQUEUE QMgrName.** UACC(NONE)
PERMIT QMgrName.** CLASS(MQQUEUE) ID(GroupName) ACCESS(READ)
RDEFINE MXTOPIC QMgrName.** UACC(NONE)
PERMIT QMgrName.** CLASS(MXTOPIC) ID(GroupName) ACCESS(READ)
RDEFINE MQPROC QMgrName.** UACC(NONE)
PERMIT QMgrName.** CLASS(MQPROC) ID(GroupName) ACCESS(READ)
RDEFINE MQNLIST QMgrName.** UACC(NONE)
PERMIT QMgrName.** CLASS(MQNLIST) ID(GroupName) ACCESS(READ)
RDEFINE MQCONN QMgrName.BATCH UACC(NONE)
PERMIT QMgrName.BATCH CLASS(MQCONN) ID(GroupName) ACCESS(READ)
RDEFINE MQCONN QMgrName.CICS UACC(NONE)
PERMIT QMgrName.CICS CLASS(MQCONN) ID(GroupName) ACCESS(READ)
RDEFINE MQCONN QMgrName.IMS UACC(NONE)
PERMIT QMgrName.IMS CLASS(MQCONN) ID(GroupName) ACCESS(READ)
```

```
RDEFINE MQCONN QMgrName.CHIN UACC(NONE)
PERMIT QMgrName.CHIN CLASS(MQCONN) ID(GroupName) ACCESS(READ)
```

Názvy proměnných mají následující význam:

QMgrName
Název správce front.

z/OS V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.

GroupName
Název skupiny, které má být udělen přístup.

Udělení úplného administrativního přístupu ke všem prostředkům ve správci front

Udělte úplný administrativní přístup ke všem prostředkům ve správci front každému uživateli nebo skupině uživatelů s obchodní potřebou.

Informace o této úloze

Můžete použít průvodce Přidat oprávnění založená na rolích nebo odpovídající příkazy pro váš operační systém.

Na platformách Multiplatforms můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Notes: ALW

1. Používáte-li produkt **runmqsc** k administraci správce front místo správce front IBM MQ Explorer, musíte udělit oprávnění k dotazování, získávání a procházení systému SYSTEM.MQSC.REPLY.QUEUEa nemusíte udělovat žádná oprávnění k systému SYSTEM.MQEXPLORER.REPLY.MODEL .
2. Při poskytování uživatelského přístupu ke všem prostředkům ve správci front existují příkazy, které uživatel nemůže spustit, pokud nemá přístup pro čtení k souboru `qm.ini` . To je způsobeno omezeními pro uživatele, kteří nejsou uživateli `mqm` , kteří mohou číst soubor `qm.ini` .

   Uživatel nemůže zadat následující příkazy, pokud mu neudělíte přístup pro čtení k souboru qm.ini :

   - Definování kanálu, který je konfigurován pro použití TLS
   - Definování kanálu pomocí proměnných automatické konfigurace definovaných v souboru `qm.ini`

Procedura

- Pokud používáte průvodce, v podokně IBM MQ Explorer Navigator klepněte pravým tlačítkem myši na správce front a klepněte na volbu **Oprávnění objektu** > **Přidat oprávnění založená na rolích**.

  Otevře se průvodce Přidat oprávnění založená na rolích.

- Linux AIX

  V systémech AIX and Linux zadejte následující příkazy:

```
setmqaut -m QMgrName -n '**' -t queue -g GroupName +alladm +browse
setmqaut -m QMgrName -n @class -t queue -g GroupName +crt
setmqaut -m QMgrName -n SYSTEM.ADMIN.COMMAND.QUEUE -t queue -g GroupName +dsp +inq +put
setmqaut -m QMgrName -n SYSTEM.MQEXPLORER.REPLY.MODEL -t queue -g GroupName +dsp +inq +get +put
setmqaut -m QMgrName -n '**' -t topic -g GroupName +alladm
setmqaut -m QMgrName -n @class -t topic -g GroupName +crt
setmqaut -m QMgrName -n '**' -t channel -g GroupName +alladm
setmqaut -m QMgrName -n @class -t channel -g GroupName +crt
setmqaut -m QMgrName -n '**' -t clntconn -g GroupName +alladm
setmqaut -m QMgrName -n @class -t clntconn -g GroupName +crt
setmqaut -m QMgrName -n '**' -t authinfo -g GroupName +alladm
setmqaut -m QMgrName -n @class -t authinfo -g GroupName +crt
setmqaut -m QMgrName -n '**' -t listener -g GroupName +alladm
setmqaut -m QMgrName -n @class -t listener -g GroupName +crt
setmqaut -m QMgrName -n '**' -t namelist -g GroupName +alladm
setmqaut -m QMgrName -n @class -t namelist -g GroupName +crt
setmqaut -m QMgrName -n '**' -t process -g GroupName +alladm
```

```
setmqaut -m QMgrName -n @class -t process -g GroupName +crt
setmqaut -m QMgrName -n '**' -t service -g GroupName +alladm
setmqaut -m QMgrName -n @class -t service -g GroupName +crt
setmqaut -m QMgrName -t qmgr -g GroupName +alladm +connect
```

Další informace viz **setmqaut** . @class

- Windows

  Pro systémy Windows zadejte stejné příkazy jako pro systémy AIX and Linux , ale použijte název profilu @CLASS místo @class.

- IBM i

  Pro systém IBM izadejte následující příkaz:

```
GRTMQMAUT OBJ(*ALL) OBJTYPE(*ALL) USER(' GroupName ') AUT(*ALLADM) MQMNAME(' QMgrName ')
```

- z/OS

  Pro systém z/OSzadejte následující příkazy:

```
RDEFINE MQADMIN QMgrName.*.** UACC(NONE)
PERMIT QMgrName.*.** CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

  Názvy proměnných mají následující význam:

  QMgrName
  Název správce front.

  z/OS V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.

  GroupName
  Název skupiny, které má být udělen přístup.

Odebrání konektivity ke správci front

Pokud nechcete, aby se uživatelské aplikace připojovaly ke správci front, odeberte jejich oprávnění pro připojení k němu.

Informace o této úloze

Pomocí příslušného příkazu pro váš operační systém odeberte oprávnění všech uživatelů pro připojení ke správci front.

V systému Multiplatformsmůžete také použít příkaz DELETE AUTHREC .

Poznámka: V systému IBM MQ Appliance můžete použít pouze příkaz **DELETE AUTHREC** .

Procedura

- ALW

  Pro systémy AIX, Linux, and Windows zadejte následující příkaz:

```
setmqaut -m QMgrName -t qmgr -g GroupName -connect
```

- IBM i

  Pro systém IBM izadejte následující příkaz:

```
RVKMQMAUT OBJ ('QMgrName') OBJTYPE(*MQM) USER(*ALL) AUT(*CONNECT)
```

- z/OS

  Pro systém z/OSzadejte následující příkazy:

```
RDEFINE MQCONN QMgrName.BATCH UACC(NONE)
RDEFINE MQCONN QMgrName.CHIN UACC(NONE)
RDEFINE MQCONN QMgrName.CICS UACC(NONE)
RDEFINE MQCONN QMgrName.IMS UACC(NONE)
```

Nezadávejte žádné příkazy PERMIT.

Názvy proměnných mají následující význam:

QMgrName
Název správce front.

z/OS V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.

GroupName
Název skupiny, které má být odepřen přístup.

Povolení připojení uživatelských aplikací ke správci front

Chcete povolit připojení uživatelské aplikace ke správci front. Pomocí tabulek v tomto tématu určete, jaké akce se mají provést.

Nejprve určete, zda se budou klientské aplikace připojovat ke správci front.

Pokud žádná z aplikací, které se budou připojovat ke správci front, nejsou klientské aplikace, zakažte vzdálený přístup podle popisu v části “Zakázání vzdáleného přístupu ke správci front” na stránce 409.

Pokud se jedna nebo více aplikací, které se budou připojovat ke správci front, jedná o klientské aplikace, zabezpečte vzdálenou konektivitu podle popisu v části “Zabezpečení vzdálené konektivity ke správci front” na stránce 402.

V obou případech nastavte zabezpečení připojení podle popisu v části “Nastavení zabezpečení připojení” na stránce 409 .

Chcete-li řídit přístup k prostředkům pro každého uživatele, který se připojuje ke správci front, postupujte podle následující tabulky. Je-li příkaz v prvním sloupci pravdivý, proveďte akci uvedenou ve druhém sloupci.

Příkaz	Provést tuto akci
Máte aplikace, které využívají fronty	Viz “Řízení uživatelského přístupu k frontám” na stránce 410
Máte aplikace, které využívají témata	Viz “Řízení uživatelského přístupu k tématům” na stránce 416.
Máte aplikace, které se dotazují na objekt správce front.	Viz “Udělení oprávnění k dotazování na správce front” na stránce 417.
Máte aplikace, které používají objekty procesu	Viz “Udělení oprávnění pro přístup k procesům” na stránce 418
Máte aplikace, které používají seznamy názvů	Viz “Udělení oprávnění pro přístup k seznamům názvů” na stránce 418

Zabezpečení vzdálené konektivity ke správci front

Vzdálenou konektivitu ke správci front můžete zabezpečit pomocí protokolu TLS, uživatelské procedury zabezpečení, záznamů ověřování kanálu nebo kombinace těchto metod.

Informace o této úloze

Klienta lze připojit ke správci front pomocí kanálu připojení klienta na pracovní stanici klienta a kanálu připojení serveru na serveru. Zabezpečte taková připojení jedním z následujících způsobů.

Postup

1. Použití TLS se záznamy ověření kanálu:
   a) Zabránit jakémukoli rozlišujícímu názvu (DN) v otevření kanálu pomocí záznamu ověřování kanálu SSLPEERMAP pro mapování všech DN na USERSRC (NOACCESS).
   b) Povolit určitým DN nebo sadám DN otevřít kanál pomocí záznamu ověření kanálu SSLPEERMAP pro jejich mapování na USERSRC (CHANNEL).
2. Použití TLS s uživatelskou procedurou pro zabezpečení zprávy:
   a) Nastavte uživatele MCAUSER v kanálu připojení serveru na identifikátor uživatele bez oprávnění.
   b) Zapište uživatelskou proceduru pro zabezpečení zprávy, abyste přiřadili hodnotu MCAUSER v závislosti na hodnotě DN TLS, které obdrží v polích SSLPeerNamePtr a SSLPeerNameLength předaných uživatelské proceduře ve struktuře MQCD.
3. Použití protokolu TLS s pevnými hodnotami definice kanálu:
   a) Nastavte SSLPEER v kanálu připojení serveru na specifickou hodnotu nebo úzký rozsah hodnot.
   b) Nastavte MCAUSER v kanálu připojení serveru na ID uživatele, se kterým má být kanál spuštěn.
4. Použití záznamů ověřování kanálu na kanálech, které nepoužívají protokol TLS:
   a) Zabraňte otevření kanálů pomocí záznamu ověřování kanálu mapování adres s adresami ADDRESS (*) a USERSRC (NOACCESS).
   b) Povolte, aby určité adresy IP otevřely kanály, a to pomocí záznamů ověřování kanálu mapování adres pro tyto adresy s USERSRC (CHANNEL).
5. Použití uživatelské procedury zabezpečení:
   a) Chcete-li autorizovat připojení na základě libovolné vlastnosti, kterou zvolíte, například původní adresy IP, napište uživatelskou proceduru pro zabezpečení zprávy.
6. Je také možné použít záznamy ověřování kanálu s uživatelskou procedurou pro zabezpečení zprávy nebo použít všechny tři metody, pokud to vaše konkrétní okolnosti vyžadují.

Blokování specifických adres IP
Můžete zabránit konkrétnímu kanálu, který přijímá příchozí připojení z adresy IP, nebo zabránit celému správci front v povolení přístupu z adresy IP pomocí záznamu ověřování kanálu.

Než začnete

Povolte záznamy ověřování kanálu spuštěním následujícího příkazu:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Informace o této úloze

Chcete-li zakázat určitým kanálům přijímat příchozí připojení a zajistit, aby byla připojení přijímána pouze při použití správného názvu kanálu, lze k blokování adres IP použít jeden typ pravidla. Chcete-li zakázat přístup adresy IP k celému správci front, měli byste obvykle k trvalému zablokování použít bránu firewall. Lze však použít jiný typ pravidla, který vám umožní dočasně blokovat několik adres, například když čekáte na aktualizaci brány firewall.

Procedura

- Chcete-li blokovat adresy IP v použití specifického kanálu, nastavte záznam ověřování kanálu pomocí příkazu MQSC **SET CHLAUTH**nebo příkazu PCF **Set Channel Authentication Record**.

```
SET CHLAUTH(generic-channel-name) TYPE(ADDRESSMAP) ADDRESS(generic-ip-address)
USERSRC(NOACCESS)
```

Příkaz má tři části:

SET CHLAUTH (*generický-název-kanálu*)
Pomocí této části příkazu můžete řídit, zda chcete blokovat připojení pro celého správce front, jeden kanál nebo rozsah kanálů. To, co zde vložíte, určuje, které oblasti jsou pokryty.

Příklad:

- SET CHLAUTH('*') -blokuje každý kanál ve správci front, tj. celý správce front.
- SET CHLAUTH ('SYSTEM. *')-blokuje každý kanál začínající na SYSTEM.
- SET CHLAUTH ('SYSTEM.DEF.SVRCONN')-blokuje kanál SYSTEM.DEF.SVRCONN

Typ pravidla CHLAUTH
Tuto část příkazu použijte k určení typu příkazu a určení, zda chcete zadat jednotlivou adresu nebo seznam adres.

Příklad:

- TYPE(ADDRESSMAP) -Použijte ADDRESSMAP, chcete-li zadat jednu adresu nebo adresu se zástupným znakem. Například ADDRESS('192.168.*') blokuje všechna připojení přicházející z adresy IP začínající na 192.168.

  Další informace o filtrování adres IP pomocí vzorů viz Generické adresy IP.
- TYPE(BLOCKADDR) -Použijte BLOCKADDR, pokud chcete dodat seznam adres, které se mají blokovat.

Další parametry
Tyto parametry závisí na typu pravidla, které jste použili v druhé části příkazu:

- Pro TYPE(ADDRESSMAP) používáte ADDRESS
- Pro TYPE(BLOCKADDR) používáte ADDRLIST

Související odkazy
NASTAVIT CHLAUTH

Dočasné blokování specifických adres IP, pokud není spuštěn správce front
V případě, že správce front není spuštěn, může být vhodné blokovat konkrétní adresy IP nebo rozsahy adres, a proto nelze zadávat příkazy MQSC. Dočasně můžete blokovat adresy IP na výjimečném základě úpravou souboru `blockaddr.ini` .

Informace o této úloze

Soubor `blockaddr.ini` obsahuje kopii definic BLOCKADDR používaných správcem front. Tento soubor načte modul listener, pokud je modul listener spuštěn před správcem front. Za těchto okolností modul listener použije všechny hodnoty, které jste ručně přidali do souboru `blockaddr.ini` .

Mějte však na paměti, že při spuštění správce front zapíše sadu definic BLOCKADDR do souboru `blockaddr.ini` a přepíše všechny případné ruční úpravy, které jste provedli. Podobně při každém přidání nebo odstranění definice BLOCKADDR pomocí příkazu **SET CHLAUTH** se aktualizuje soubor `blockaddr.ini` . Proto můžete provádět trvalé změny definic BLOCKADDR pouze pomocí příkazu **SET CHLAUTH** , když je spuštěn správce front.

Postup

1. Otevřete soubor `blockaddr.ini` v textovém editoru.
   Soubor je umístěn v datovém adresáři správce front.
2. Přidejte adresy IP jako jednoduché dvojice klíč-hodnota, kde klíčové slovo je `Addr`.
   Informace o filtrování adres IP pomocí vzorů viz Generické adresy IP.
   Příklad:

```
Addr = 192.0.2.0
```

```
Addr = 192.0.*
Addr = 192.0.2.1-8
```

Související úlohy

“Blokování specifických adres IP” na stránce 403
Můžete zabránit konkrétnímu kanálu, který přijímá příchozí připojení z adresy IP, nebo zabránit celému správci front v povolení přístupu z adresy IP pomocí záznamu ověřování kanálu.

Související odkazy

NASTAVIT CHLAUTH

Blokování specifických ID uživatelů
Můžete zabránit specifickým uživatelům v použití kanálu určením ID uživatelů, která v případě deklarace způsobí ukončení kanálu. To provedete nastavením záznamu ověřování kanálu.

Než začnete

Ujistěte se, že záznamy ověření kanálu jsou povoleny následujícím způsobem:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Postup

Nastavte záznam ověřování kanálu pomocí příkazu MQSC **SET CHLAUTH**nebo příkazu PCF **Set Channel Authentication Record**. Můžete například zadat příkaz MQSC:

```
SET CHLAUTH(' generic-channel-name ') TYPE(BLOCKUSER) USERLIST(userID1, userID2)
```

generický-název-kanálu je buď název kanálu, ke kterému chcete řídit přístup, nebo vzor obsahující symbol hvězdičky (*) jako zástupný znak, který odpovídá názvu kanálu.
Seznam uživatelů poskytovaný v systému TYPE(BLOCKUSER) se vztahuje pouze na kanály SVRCONN a nikoli na kanály správce front.
userID1 a *userID2* jsou ID uživatele, kterému má být zabráněno používat kanál. Můžete také zadat speciální hodnotu *MQADMIN , která bude odkazovat na oprávněné administrativní uživatele. Další informace o oprávněných uživatelích viz “Oprávnění uživatelé” na stránce 344. Další informace o produktu *MQADMINviz SET CHLAUTH.

Související odkazy

NASTAVIT CHLAUTH

Mapování vzdáleného správce front na ID uživatele MCAUSER
Pomocí záznamu ověřování kanálu můžete nastavit atribut MCAUSER kanálu podle správce front, ze kterého se kanál připojuje.

Než začnete

Ujistěte se, že záznamy ověření kanálu jsou povoleny následujícím způsobem:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Informace o této úloze

Volitelně můžete omezit adresy IP, na které se pravidlo vztahuje.

Všimněte si, že tato technika se nevztahuje na kanály připojení serveru. Zadáte-li název kanálu připojení serveru v následujících příkazech, nebude to mít žádný vliv.

Procedura

- Nastavte záznam ověřování kanálu pomocí příkazu MQSC **SET CHLAUTH**nebo příkazu PCF **Set Channel Authentication Record**. Můžete například zadat příkaz MQSC:

```
SET CHLAUTH(' generic-channel-name ') TYPE (QMGRMAP) QMNAME(generic-partner-qmgr-name
) USERSRC(MAP) MCAUSER(user)
```

  generický-název-kanálu je buď název kanálu, ke kterému chcete řídit přístup, nebo vzor obsahující symbol hvězdičky (*) jako zástupný znak, který odpovídá názvu kanálu.
  generic-partner-qmgr-name je buď název správce front, nebo vzor obsahující symbol hvězdičky (*) jako zástupný znak, který odpovídá názvu správce front.
  user je ID uživatele, které má být použito pro všechna připojení ze zadaného správce front.

- Chcete-li tento příkaz omezit na určité adresy IP, zadejte následující parametr **ADDRESS** :

```
SET CHLAUTH(' generic-channel-name ') TYPE (QMGRMAP) QMNAME(generic-partner-qmgr-name
) USERSRC(MAP) MCAUSER(user) ADDRESS(
generic-ip-address)
```

  generický-název-kanálu je buď název kanálu, ke kterému chcete řídit přístup, nebo vzor obsahující symbol hvězdičky (*) jako zástupný znak, který odpovídá názvu kanálu.
  generic-ip-address je buď jedna adresa, nebo vzor obsahující symbol hvězdičky (*) jako zástupný znak, nebo spojovník (-) označující rozsah, který odpovídá adrese. Další informace o generických adresách IP naleznete v tématu Generické adresy IP.

Související odkazy
NASTAVIT CHLAUTH

Mapování ID uživatele klienta na ID uživatele MCAUSER
Pomocí záznamu ověřování kanálu můžete změnit atribut MCAUSER kanálu připojení serveru podle ID uživatele přijatého od klienta.

Než začnete
Ujistěte se, že záznamy ověření kanálu jsou povoleny následujícím způsobem:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Informace o této úloze
Všimněte si, že tato technika platí pouze pro kanály připojení serveru. Nemá žádný vliv na jiné typy kanálů.

Postup

Nastavte záznam ověřování kanálu pomocí příkazu MQSC **SET CHLAUTH**nebo příkazu PCF **Set Channel Authentication Record** . Můžete například zadat příkaz MQSC:

```
SET CHLAUTH(' generic-channel-name ') TYPE (USERMAP) CLNTUSER(client-user-name) USERSRC(MAP)
MCAUSER(
user)
```

generický-název-kanálu je buď název kanálu, ke kterému chcete řídit přístup, nebo vzor obsahující symbol hvězdičky (*) jako zástupný znak, který odpovídá názvu kanálu.
jméno-uživatele klienta je ID uživatele přidružené k připojení klienta. Hodnotu lze uplatnit v klientské aplikaci a změnit ověřením připojení pomocí předčasného převzetí nebo nastavení prostřednictvím uživatelské procedury kanálu.
user je ID uživatele, které se má použít místo jména uživatele klienta.

Související odkazy
NASTAVIT CHLAUTH
Atributy sekce kanálů (ChlauthEarlyAdopt)

Mapování rozlišujícího názvu SSL nebo TLS na ID uživatele MCAUSER
Pomocí záznamu ověřování kanálu můžete nastavit atribut MCAUSER kanálu podle přijatého rozlišujícího názvu (DN).

Než začnete
Ujistěte se, že záznamy ověření kanálu jsou povoleny následujícím způsobem:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Postup
Nastavte záznam ověřování kanálu pomocí příkazu MQSC **SET CHLAUTH**nebo příkazu PCF **Set Channel Authentication Record**. Můžete například zadat příkaz MQSC:

```
SET CHLAUTH('generic-channel-name') TYPE (SSLPEERMAP)
SSLPEER(generic-ssl-peer-name) SSLCERTI(generic-issuer-name)
USERSRC(MAP) MCAUSER(user)
```

generický-název-kanálu je buď název kanálu, ke kterému chcete řídit přístup, nebo vzor obsahující symbol hvězdičky (*) jako zástupný znak, který odpovídá názvu kanálu.
generic-ssl-peer-name je řetězec, který odpovídá standardním pravidlům IBM MQ pro hodnoty SSLPEER. Viz IBM MQ pravidla pro hodnoty SSLPEER.
user je ID uživatele, které se má použít pro všechna připojení používající uvedené DN.
generický-název-vydavatele odkazuje na DN vydavatele certifikátu, který se má shodovat. Tento parametr je volitelný, ale měli byste jej použít, abyste se vyhnuli nápadnému porovnávání nesprávného certifikátu, pokud se používá více certifikačních autorit.

Související odkazy
NASTAVIT CHLAUTH

Blokování přístupu ze vzdáleného správce front
Záznam ověřování kanálu můžete použít k tomu, abyste zabránili vzdálenému správci front ve spouštění kanálů.

Než začnete
Ujistěte se, že záznamy ověření kanálu jsou povoleny následujícím způsobem:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Informace o této úloze
Všimněte si, že tato technika se nevztahuje na kanály připojení serveru. Zadáte-li název kanálu připojení serveru v následujícím příkazu, nebude to mít žádný vliv.

Postup
Nastavte záznam ověřování kanálu pomocí příkazu MQSC **SET CHLAUTH**nebo příkazu PCF **Set Channel Authentication Record**. Můžete například zadat příkaz MQSC:

```
SET CHLAUTH(' generic-channel-name ') TYPE(QMGRMAP) QMNAME(' generic-partner-qmgr-name ')
USERSRC(NOACCESS)
```

generický-název-kanálu je buď název kanálu, ke kterému chcete řídit přístup, nebo vzor obsahující symbol hvězdičky (*) jako zástupný znak, který odpovídá názvu kanálu.

generic-partner-qmgr-name je buď název správce front, nebo vzor obsahující symbol hvězdičky (*) jako zástupný znak, který odpovídá názvu správce front.

Související odkazy

NASTAVIT CHLAUTH

Blokování přístupu pro ID uživatele klienta

Záznam ověřování kanálu můžete použít, chcete-li zabránit ID uživatele klienta v ustanovení připojení kanálu.

Než začnete

Ujistěte se, že záznamy ověření kanálu jsou povoleny následujícím způsobem:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Informace o této úloze

Všimněte si, že tato technika platí pouze pro kanály připojení serveru. Nemá žádný vliv na jiné typy kanálů.

Postup

Nastavte záznam ověřování kanálu pomocí příkazu MQSC **SET CHLAUTH**nebo příkazu PCF **Set Channel Authentication Record**. Můžete například zadat příkaz MQSC:

```
SET CHLAUTH(' generic-channel-name ') TYPE(USERMAP) CLNTUSER(' client-user-name ')
USERSRC(NOACCESS)
```

generický-název-kanálu je buď název kanálu, ke kterému chcete řídit přístup, nebo vzor obsahující symbol hvězdičky (*) jako zástupný znak, který odpovídá názvu kanálu.

jméno-uživatele klienta je ID uživatele přidružené k připojení klienta. Hodnotu lze uplatnit v klientské aplikaci a změnit ověřením připojení pomocí předčasného převzetí nebo nastavení prostřednictvím uživatelské procedury kanálu.

Související odkazy

NASTAVIT CHLAUTH

Blokování přístupu pro rozlišující název SSL nebo TLS

Záznam ověřování kanálu můžete použít k tomu, abyste zabránili spuštění kanálů rozlišujícího názvu (DN) TLS.

Než začnete

Ujistěte se, že záznamy ověření kanálu jsou povoleny následujícím způsobem:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Postup

Nastavte záznam ověřování kanálu pomocí příkazu MQSC **SET CHLAUTH**nebo příkazu PCF **Set Channel Authentication Record**. Můžete například zadat příkaz MQSC:

```
SET CHLAUTH('generic-channel-name') TYPE(SSLPEERMAP)
SSLPEER('generic-ssl-peer-name') SSLCERTI(generic-issuer-name)
USERSRC(NOACCESS)
```

generický-název-kanálu je buď název kanálu, ke kterému chcete řídit přístup, nebo vzor obsahující symbol hvězdičky (*) jako zástupný znak, který odpovídá názvu kanálu.

generic-ssl-peer-name je řetězec, který odpovídá standardním pravidlům IBM MQ pro hodnoty SSLPEER. Viz IBM MQ pravidla pro hodnoty SSLPEER.

generický-název-vydavatele odkazuje na DN vydavatele certifikátu, který se má shodovat. Tento parametr je volitelný, ale měli byste jej použít, abyste se vyhnuli nápadnému porovnávání nesprávného certifikátu, pokud se používá více certifikačních autorit.

Související odkazy

NASTAVIT CHLAUTH

Mapování adresy IP na ID uživatele MCAUSER

Pomocí záznamu ověřování kanálu můžete nastavit atribut MCAUSER kanálu podle adresy IP, ze které je připojení přijímáno.

Než začnete

Ujistěte se, že záznamy ověření kanálu jsou povoleny následujícím způsobem:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Postup

Nastavte záznam ověřování kanálu pomocí příkazu MQSC **SET CHLAUTH**nebo příkazu PCF **Set Channel Authentication Record**. Můžete například zadat příkaz MQSC:

```
SET CHLAUTH(' generic-channel-name ') TYPE(ADDRESSMAP) ADDRESS(' generic-ip-address ')
USERSRC(MAP) MCAUSER(user)
```

generický-název-kanálu je buď název kanálu, ke kterému chcete řídit přístup, nebo vzor obsahující symbol hvězdičky (*) jako zástupný znak, který odpovídá názvu kanálu.

user je ID uživatele, které se má použít pro všechna připojení používající uvedené DN.

generic-ip-address je buď adresa, ze které se provádí připojení, nebo vzor obsahující hvězdičku (*) jako zástupný znak nebo pomlčku (-) označující rozsah, který se shoduje s adresou.

Související odkazy

NASTAVIT CHLAUTH

Zakázání vzdáleného přístupu ke správci front

Pokud nechcete, aby se klientské aplikace připojovaly ke správci front, zakažte k němu vzdálený přístup.

Informace o této úloze

Zamezte připojení aplikací klienta ke správci front jedním z následujících způsobů:

Procedura

- Odstraňte všechny kanály připojení serveru pomocí příkazu MQSC **DELETE CHANNEL**.
- Pomocí příkazu MQSC **ALTER CHANNEL**nastavte identifikátor uživatele agenta kanálu zpráv (MCAUSER) kanálu na ID uživatele bez přístupových práv.

Nastavení zabezpečení připojení

Udělte oprávnění pro připojení ke správci front každému uživateli nebo skupině uživatelů s obchodní potřebou tak učinit.

Informace o této úloze

Chcete-li nastavit zabezpečení připojení, použijte příslušné příkazy pro váš operační systém.

Na platformách Multiplatforms můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Procedura

- ALW

  V systému AIX, Linux, and Windows:

  ```
  setmqaut -m QMgrName -t qmgr -g GroupName +connect
  ```

- IBM i

  V systému IBM i:

  ```
  GRTMQMAUT OBJ('QMgrName') OBJTYPE(*MQM) USER('GroupName') AUT(*CONNECT)
  ```

- z/OS

  V systému z/OS:

  ```
  RDEFINE MQCONN QMgrName.BATCH UACC(NONE)
  PERMIT QMgrName.BATCH CLASS(MQCONN) ID(GroupName) ACCESS(READ)
  RDEFINE MQCONN QMgrName.CICS UACC(NONE)
  PERMIT QMgrName.CICS CLASS(MQCONN) ID(GroupName) ACCESS(READ)
  RDEFINE MQCONN QMgrName.IMS UACC(NONE)
  PERMIT QMgrName.IMS CLASS(MQCONN) ID(GroupName) ACCESS(READ)
  RDEFINE MQCONN QMgrName.CHIN UACC(NONE)
  PERMIT QMgrName.CHIN CLASS(MQCONN) ID(GroupName) ACCESS(READ)
  ```

  Tyto příkazy poskytují oprávnění k připojení pro dávku CICS, IMS a inicializátor kanálu (CHIN). Pokud nepoužijete konkrétní typ připojení, vynechte příslušné příkazy.

  Názvy proměnných mají následující význam:

  QMgrName
  Název správce front. V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.

  ObjectProfile
  Název objektu nebo generického profilu, pro který se mají změnit autorizace.

  GroupName
  Název skupiny, které má být udělen přístup.

Související pojmy

“Profily zabezpečení připojení pro inicializátor kanálu” na stránce 200
Profily pro kontrolu připojení z inicializátoru kanálu se skládají z názvu správce front nebo skupiny sdílení front následovaného slovem *CHIN*. Přidělte ID uživatele, které používá adresní prostor spuštěné úlohy inicializátoru kanálu, přístup READ k profilu připojení.

Řízení uživatelského přístupu k frontám

Chcete řídit přístup aplikací k frontám. Toto téma slouží k určení akcí, které mají být provedeny.

Pro každý pravdivý příkaz v prvním sloupci proveďte akci uvedenou ve druhém sloupci.

Příkaz	Akce
Aplikace získává zprávy z fronty	Viz “Udělení oprávnění k získání zpráv z front” na stránce 411
Aplikace nastavuje kontext	Viz “Udělení oprávnění k nastavení kontextu” na stránce 411
Aplikace předává kontext	Viz “Udělení oprávnění k předání kontextu” na stránce 412

Příkaz	Akce
Aplikace vkládá zprávy do klastrované fronty.	Viz “Autorizace vkládání zpráv do front vzdáleného klastru” na stránce 496
Aplikace vkládá zprávy do lokální fronty	Viz “Udělení oprávnění pro vložení zpráv do lokální fronty” na stránce 413
Aplikace vkládá zprávy do modelové fronty	Viz “Udělení oprávnění pro vložení zpráv do modelové fronty” na stránce 414
Aplikace vkládá zprávy do vzdálené fronty	Viz “Udělení oprávnění pro vložení zpráv do fronty vzdáleného klastru” na stránce 415

Udělení oprávnění k získání zpráv z front
Udělte oprávnění k získávání zpráv z fronty nebo sady front pro každou skupinu uživatelů s obchodní potřebou.

Informace o této úloze

Chcete-li udělit oprávnění k získání zpráv z některých front, použijte odpovídající příkazy pro váš operační systém.

Na platformách Multiplatforms můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Procedura

- Pro systémy AIX, Linux, and Windows zadejte následující příkaz:

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +get
```

- Pro systém IBM izadejte následující příkaz:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*GET) MQMNAME(' QMgrName ')
```

- Pro systém z/OSzadejte následující příkazy:

```
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(UPDATE)
```

Názvy proměnných mají následující význam:

QMgrName
Název správce front. V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.

ObjectProfile
Název objektu nebo generického profilu, pro který se mají změnit autorizace.

GroupName
Název skupiny, které má být udělen přístup.

Udělení oprávnění k nastavení kontextu
Udělte oprávnění k nastavení kontextu pro vkládané zprávy každé skupině uživatelů s obchodní potřebou.

Informace o této úloze

Chcete-li udělit oprávnění k nastavení kontextu v některých frontách, použijte příslušné příkazy pro váš operační systém.

Na platformách Multiplatforms můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Procedura

- Pro systémy AIX, Linux, and Windows zadejte jeden z následujících příkazů:
  - Chcete-li nastavit pouze kontext identity, postupujte takto:

    ```
    setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +setid
    ```

  - Chcete-li nastavit celý kontext, postupujte takto:

    ```
    setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +setall
    ```

  Poznámka: Chcete-li použít oprávnění `setid` nebo `setall` , musí být autorizace uděleny jak pro příslušný objekt fronty, tak pro objekt správce front.
- Pro systém IBM izadejte jeden z následujících příkazů:
  - Chcete-li nastavit pouze kontext identity, postupujte takto:

    ```
    GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*SETID) MQMNAME('
    QMgrName ')
    ```

  - Chcete-li nastavit celý kontext, postupujte takto:

    ```
    GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*SETALL) MQMNAME('
    QMgrName ')
    ```

- Pro systém z/OSzadejte jednu z následujících sad příkazů:
  - Chcete-li nastavit pouze kontext identity, postupujte takto:

    ```
    RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
    PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
    ```

  - Chcete-li nastavit celý kontext, postupujte takto:

    ```
    RDEFINE MQQUEUE QMgrName. ObjectProfile UACC(NONE)
    PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(CONTROL)
    ```

  Názvy proměnných mají následující význam:

  QMgrName
  Název správce front. V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.

  ObjectProfile
  Název objektu nebo generického profilu, pro který se mají změnit autorizace.

  GroupName
  Název skupiny, které má být udělen přístup.

Udělení oprávnění k předání kontextu
Udělte oprávnění k předání kontextu z načtené zprávy do vkládané zprávy každé skupině uživatelů s obchodní potřebou.

Informace o této úloze

Chcete-li udělit oprávnění k předávání kontextu v některých frontách, použijte odpovídající příkazy pro váš operační systém.

Na platformách Multiplatforms můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Procedura

- ALW

  Pro systémy AIX, Linux, and Windows zadejte jeden z následujících příkazů:

  - Chcete-li předat pouze kontext identity, postupujte takto:

    ```
    setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +passid
    ```

  - Chcete-li předat celý kontext, postupujte takto:

    ```
    setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +passall
    ```

- IBM i

  Pro systém IBM izadejte jeden z následujících příkazů:

  - Chcete-li předat pouze kontext identity, postupujte takto:

    ```
    GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*PASSID) MQMNAME('
    QMgrName ')
    ```

  - Chcete-li předat celý kontext, postupujte takto:

    ```
    GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*PASSALL) MQMNAME('
    QMgrName ')
    ```

- z/OS

  Pro systém z/OSzadejte následující příkazy pro předání kontextu identity nebo celého kontextu:

  ```
  RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
  PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
  ```

  Názvy proměnných mají následující význam:

  QMgrName
  Název správce front. V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.

  ObjectProfile
  Název objektu nebo generického profilu, pro který se mají změnit autorizace.

  GroupName
  Název skupiny, které má být udělen přístup.

Udělení oprávnění pro vložení zpráv do lokální fronty
Udělte oprávnění vkládat zprávy do lokální fronty nebo sady front pro každou skupinu uživatelů s obchodní potřebou.

Informace o této úloze

Chcete-li udělit oprávnění k vkládání zpráv do některých lokálních front, použijte odpovídající příkazy pro váš operační systém.

Na platformách Multiplatforms můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Procedura

- Pro systémy AIX, Linux, and Windows zadejte následující příkaz:

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +put
```

- Pro systém IBM izadejte následující příkaz:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*PUT) MQMNAME(' QMgrName ')
```

- Pro systém z/OSzadejte následující příkazy:

```
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
```

Názvy proměnných mají následující význam:

QMgrName
Název správce front. V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.

ObjectProfile
Název objektu nebo generického profilu, pro který se mají změnit autorizace.

GroupName
Název skupiny, které má být udělen přístup.

Udělení oprávnění pro vložení zpráv do modelové fronty
Udělte oprávnění vkládat zprávy do modelové fronty nebo sady modelových front každé skupině uživatelů s obchodní potřebou.

Informace o této úloze

Modelové fronty se používají k vytváření dynamických front. Proto musíte udělit oprávnění pro modelové i dynamické fronty. Chcete-li udělit tato oprávnění, použijte odpovídající příkazy pro váš operační systém.

Na platformách Multiplatforms můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Procedura

- V systémech AIX, Linux, and Windows zadejte následující příkazy:

```
setmqaut -m QMgrName -n ModelQueueName -t queue -g GroupName +put
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +put
```

- Pro systém IBM izadejte následující příkazy:

```
GRTMQMAUT OBJ(' ModelQueueName ') OBJTYPE(*Q) USER(GroupName) AUT(*PUT) MQMNAME(' QMgrName ')
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*PUT) MQMNAME(' QMgrName ')
```

- Pro systém z/OSzadejte následující příkazy:

```
RDEFINE MQQUEUE QMgrName.ModelQueueName UACC(NONE)
PERMIT QMgrName.ModelQueueName CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
```

Názvy proměnných mají následující význam:

QMgrName
Název správce front. V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.

Název ModelQueue
Název modelové fronty, na které jsou založeny dynamické fronty.

ObjectProfile
Název dynamické fronty nebo generického profilu, pro který se mají změnit autorizace.

GroupName
Název skupiny, které má být udělen přístup.

Udělení oprávnění pro vložení zpráv do fronty vzdáleného klastru
Udělte oprávnění vkládat zprávy do vzdálené fronty klastru nebo do sady front pro každou skupinu uživatelů s obchodní potřebou.

Informace o této úloze

Chcete-li vložit zprávu do fronty vzdáleného klastru, můžete ji buď vložit do lokální definice vzdálené fronty, nebo do plně kvalifikované vzdálené fronty. Pokud používáte lokální definici vzdálené fronty, potřebujete oprávnění k vložení do lokálního objektu: viz “Udělení oprávnění pro vložení zpráv do lokální fronty” na stránce 413. Používáte-li plně kvalifikovanou vzdálenou frontu, potřebujete oprávnění k vložení do vzdálené fronty. Udělte toto oprávnění pomocí příslušných příkazů pro váš operační systém.

Výchozí chování je provádět řízení přístupu vůči serveru `SYSTEM.CLUSTER.TRANSMIT.QUEUE`. Všimněte si, že toto chování platí i v případě, že používáte více přenosových front.

Specifické chování popsané v tomto tématu platí pouze v případě, že jste nakonfigurovali atribut **`ClusterQueueAccessControl`** v souboru `qm.ini` na hodnotu *RQMName*, jak je popsáno v tématu Sekce zabezpečení , a restartovali správce front.

Na platformách Multiplatforms můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Procedura

- Pro systémy AIX, Linux, and Windows zadejte následující příkaz:

```
setmqaut -m QMgrName -t rqmname -n
ObjectProfile -g GroupName +put
```

  Všimněte si, že objekt *rqmname* můžete použít pouze pro fronty vzdáleného klastru.
- Pro systém IBM izadejte následující příkaz:

```
GRTMQMAUT OBJTYPE(*RMTMQMNAME) OBJ('
ObjectProfile') USER(GroupName) AUT(*PUT) MQMNAME('
QMgrName')
```

  Všimněte si, že můžete použít objekt RMTMQMNAME pouze pro fronty vzdáleného klastru.
- Pro systém z/OSzadejte následující příkazy:

```
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
```

  Všimněte si, že název vzdáleného správce front (nebo skupiny sdílení front) můžete použít pouze pro fronty vzdáleného klastru.

  Názvy proměnných mají následující význam:

  QMgrName
  Název správce front. V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.

  ObjectProfile
  Název vzdáleného správce front nebo generického profilu, pro který se mají změnit autorizace.

GroupName
Název skupiny, které má být udělen přístup.

Řízení uživatelského přístupu k tématům

Musíte řídit přístup aplikací k tématům. Toto téma slouží k určení akcí, které mají být provedeny.

Pro každý pravdivý příkaz v prvním sloupci proveďte akci uvedenou ve druhém sloupci.

Tabulka 74. Řízení uživatelského přístupu k tématům

Příkaz	**Akce**
Aplikace publikuje zprávy do tématu	Viz “Udělení oprávnění k publikování zpráv do tématu” na stránce 416
Aplikace se přihlásí k odběru tématu	Viz “Udělení oprávnění k odběru témat” na stránce 416

Udělení oprávnění k publikování zpráv do tématu
Udělte oprávnění k publikování zpráv pro téma nebo sadu témat, pro každou skupinu uživatelů s obchodní potřebou.

Informace o této úloze

Chcete-li udělit oprávnění k publikování zpráv pro některá témata, použijte odpovídající příkazy pro váš operační systém.

Na platformách Multiplatforms můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Procedura

- Pro systémy AIX, Linux, and Windows zadejte následující příkaz:

```
setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName +pub
```

- Pro systém IBM izadejte následující příkaz:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*TOPIC) USER(GroupName) AUT(*PUB) MQMNAME('
QMgrName ')
```

- Pro systém z/OSzadejte následující příkazy:

```
RDEFINE MQTOPIC QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQTOPIC) ID(GroupName) ACCESS(UPDATE)
```

Názvy proměnných mají následující význam:

QMgrName
Název správce front. V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.

ObjectProfile
Název objektu nebo generického profilu, pro který se mají změnit autorizace.

GroupName
Název skupiny, které má být udělen přístup.

Udělení oprávnění k odběru témat
Udělte oprávnění k přihlášení k odběru tématu nebo sady témat pro každou skupinu uživatelů s obchodní potřebou.

Informace o této úloze

Chcete-li udělit oprávnění k odběru některých témat, použijte odpovídající příkazy pro váš operační systém.

Na platformách Multiplatforms můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Procedura

- Pro systémy AIX, Linux, and Windows zadejte následující příkaz:

```
setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName +sub
```

- Pro systém IBM izadejte následující příkaz:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*TOPIC) USER(GroupName) AUT(*SUB) MQMNAME('
QMgrName ')
```

- Pro systém z/OSzadejte následující příkazy:

```
RDEFINE MQTOPIC QMgrName.SUBSCRIBE.ObjectProfile UACC(NONE)
PERMIT QMgrName.SUBSCRIBE.ObjectProfile CLASS(MQTOPIC) ID(GroupName) ACCESS(UPDATE)
```

Názvy proměnných mají následující význam:

QMgrName
Název správce front. V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.

ObjectProfile
Název objektu nebo generického profilu, pro který se mají změnit autorizace.

GroupName
Název skupiny, které má být udělen přístup.

Udělení oprávnění k dotazování na správce front

Udělte oprávnění k dotazování na správce front pro každou skupinu uživatelů, pro kterou je obchodní potřeba.

Informace o této úloze

Chcete-li udělit oprávnění k dotazování na správce front, použijte příslušné příkazy pro váš operační systém.

Na platformách Multiplatforms můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Procedura

- Pro systémy AIX, Linux, and Windows zadejte následující příkaz:

```
setmqaut -m QMgrName -n ObjectProfile -t qmgr -g GroupName +inq
```

- Pro systém IBM izadejte následující příkaz:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*MQM) USER(GroupName) AUT(*INQ) MQMNAME(' QMgrName
')
```

- Pro systém z/OSzadejte následující příkazy:

```
RDEFINE MQCMDS QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

Tyto příkazy udělují přístup k určenému správci front. Chcete-li uživateli povolit použití příkazu MQINQ, zadejte následující příkazy:

```
RDEFINE MQCMDS QMgrName.MQINQ.QMGR UACC(NONE)
PERMIT QMgrName.MQINQ.QMGR CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

Názvy proměnných mají následující význam:

QMgrName
Název správce front. V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.

ObjectProfile
Název objektu nebo generického profilu, pro který se mají změnit autorizace.

GroupName
Název skupiny, které má být udělen přístup.

Udělení oprávnění pro přístup k procesům

Udělte oprávnění pro přístup k procesu nebo sadě procesů každé skupině uživatelů s obchodní potřebou.

Informace o této úloze

Chcete-li udělit oprávnění pro přístup k některým procesům, použijte odpovídající příkazy pro váš operační systém.

Na platformách Multiplatforms můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Procedura

- Pro systémy AIX, Linux, and Windows zadejte následující příkaz:

```
setmqaut -m QMgrName -n ObjectProfile -t process -g GroupName +all
```

- Pro systém IBM izadejte následující příkaz:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*PRC) USER(GroupName) AUT(*ALL) MQMNAME(' QMgrName
')
```

- Pro systém z/OSzadejte následující příkazy:

```
RDEFINE MQPROC QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQPROC) ID(GroupName) ACCESS(READ)
```

Názvy proměnných mají následující význam:

QMgrName
Název správce front. V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.

ObjectProfile
Název objektu nebo generického profilu, pro který se mají změnit autorizace.

GroupName
Název skupiny, které má být udělen přístup.

Udělení oprávnění pro přístup k seznamům názvů

Udělte oprávnění pro přístup k seznamu názvů nebo sadě seznamů názvů každé skupině uživatelů s obchodní potřebou.

Informace o této úloze

Chcete-li udělit oprávnění pro přístup k některým seznamům názvů, použijte příslušné příkazy pro váš operační systém.

Na platformách Multiplatforms můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Procedura

- Pro systémy AIX, Linux, and Windows zadejte následující příkaz:

```
setmqaut -m QMgrName -n
ObjectProfile -t namelist -g GroupName
+all
```

- Pro systém IBM izadejte následující příkaz:

```
GRTMQMAUT OBJ('ObjectProfile
') OBJTYPE(*NMLIST) USER(GroupName) AUT(*ALL) MQMNAME('
QMgrName')
```

- Pro systém z/OSzadejte následující příkazy:

```
RDEFINE MQNLIST
QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile
CLASS(MQNLIST) ID(GroupName) ACCESS(READ)
```

  Názvy proměnných mají následující význam:

  QMgrName
  Název správce front. V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.

  ObjectProfile
  Název objektu nebo generického profilu, pro který se mají změnit autorizace.

  GroupName
  Název skupiny, které má být udělen přístup.

ALW Oprávnění ke správě IBM MQ v systému AIX, Linux, and Windows

Administrátoři produktu IBM MQ mohou použít všechny příkazy produktu IBM MQ a udělit oprávnění ostatním uživatelům. Když administrátoři zadávají příkazy pro vzdálené správce front, musí mít požadované oprávnění pro vzdáleného správce front. Další aspekty platí pro systémy Windows .

Administrátoři systému IBM MQ mají oprávnění používat všechny příkazy systému IBM MQ (včetně příkazů pro udělení oprávnění systému IBM MQ ostatním uživatelům).

Chcete-li být administrátorem produktu IBM MQ , musíte být členem speciální skupiny, která se nazývá skupina **mqm** .

Windows Alternativně, pouze v systému Windows , mohou lokální účty spravovat produkt IBM MQ , pokud jsou členy skupiny administrátorů na systémech Windows .

Upozornění: Uživatele Azure AD můžete přidat do skupiny mqm pomocí příkazu administrátora. Použijte například příkaz `net localgroup mqm AzureAD\<your userID> /add`. Poté spusťte příkazy administrace IBM MQ nebo použijte příkaz IBM MQ Explorer.

Skupina **mqm** se vytvoří automaticky při instalaci produktu IBM MQ . Do skupiny můžete přidat další uživatele, kteří jim umožní provádět administraci. Všichni členové této skupiny mají přístup ke všem prostředkům. Tento přístup lze odvolat pouze odebráním uživatele ze skupiny **mqm** a zadáním příkazu **REFRESH SECURITY** .

Administrátoři mohou k administraci produktu IBM MQpoužívat řídicí příkazy. Jeden z těchto řídicích příkazů je **setmqaut**, který se používá k udělení oprávnění ostatním uživatelům, aby jim umožnil přístup nebo řízení prostředků IBM MQ . Příkazy PCF pro správu záznamů oprávnění jsou k dispozici pro neadministrátory, kteří mají ve správci front udělena oprávnění dsp a chg. Další informace o správě oprávnění pomocí příkazů PCF naleznete v tématu Programovatelné formáty příkazů.

Administrátoři musí mít nezbytná oprávnění pro zpracování příkazů MQSC vzdáleným správcem front. Produkt IBM MQ Explorer vydává příkazy PCF k provádění administrativních úloh. Administrátoři nepotřebují žádná další oprávnění k použití produktu IBM MQ Explorer k administraci správce front v lokálním systému. Je-li produkt IBM MQ Explorer používán k administraci správce front v jiném systému, musí mít administrátoři potřebná oprávnění pro příkazy PCF, které má vzdálený správce front zpracovat.

Upozornění: V systému IBM MQ 8.0nemusíte být administrátorem pro použití řídicího příkazu **runmqsc**, který vydává příkazy IBM MQ Script (MQSC).

Je-li produkt **runmqsc** používán v nepřímém režimu k odesílání příkazů MQSC vzdálenému správci front, je každý příkaz MQSC zapouzdřen v rámci příkazu Escape PCF.

Další informace o kontrolách oprávnění při zpracování příkazů PCF a MQSC naleznete v následujících tématech:

- Informace o příkazech PCF, které pracují se správci front, frontami, procesy, seznamy názvů a objekty ověřovacích informací, naleznete v tématu Oprávnění pro práci s IBM MQ objekty. V této části naleznete informace o ekvivalentních příkazech MQSC zapouzdřených v příkazech Escape PCF.
- Informace o příkazech PCF, které pracují na kanálech, inicializátorech kanálů, modulech listener a klastrech, naleznete v tématu Zabezpečení kanálu.
- Informace o příkazech PCF, které pracují se záznamy oprávnění, naleznete v tématu Kontrola oprávnění pro příkazy PCF .
- z/OS Informace o příkazech MQSC, které jsou zpracovány příkazovým serverem v systému IBM MQ for z/OS, naleznete v tématu Zabezpečení příkazů a zabezpečení prostředků příkazů v systému z/OS .

Na systémech Windows má navíc účet SYSTEM úplný přístup k prostředkům IBM MQ .

Na platformách AIX and Linux je také vytvořeno speciální ID uživatele **mqm** , které je určeno pouze pro použití produktem. Nesmí být nikdy k dispozici pro neprivilegované uživatele. Všechny objekty IBM MQ jsou vlastněny ID uživatele **mqm**.

V systémech Windows mohou členové skupiny Administrátoři spravovat také libovolného správce front, stejně jako účet SYSTEM. Můžete také vytvořit skupinu domény **mqm** na řadiči domény, která obsahuje všechna ID privilegovaných uživatelů aktivní v doméně, a přidat ji do lokální skupiny **mqm** . Některé příkazy, například **crtmqm**, manipulují s oprávněními na objektech IBM MQ , a proto potřebují oprávnění pro práci s těmito objekty (jak je popsáno v následujících sekcích). Členové skupiny **mqm** mají oprávnění pracovat se všemi objekty, ale v systémech Windows mohou nastat okolnosti, kdy je oprávnění odepřeno, pokud máte lokálního uživatele a uživatele s ověřenou doménou se stejným názvem. To je popsáno v tématu “Činitelé a skupiny na AIX, Linux, and Windows” na stránce 423.

Verze systému Windows s funkcí UAC (User Account Control) omezují akce, které mohou uživatelé provádět v určitých zařízeních operačního systému, a to i v případě, že jsou členy skupiny administrátorů. Pokud je vaše ID uživatele ve skupině administrátorů, ale ne ve skupině **mqm** , musíte použít zvýšený příkazový řádek k vydání příkazů IBM MQ admin, jako např. **crtmqm**, jinak se vygeneruje chyba AMQ7077: Nemáte oprávnění k provedení požadované operace . Chcete-li otevřít příkazový řádek se zvýšeným oprávněním, klepněte pravým tlačítkem myši na položku nabídky Start nebo ikonu příkazového řádku a vyberte volbu **Spustit jako administrátor**.

Nemusíte být členem skupiny **mqm** , abyste mohli provést následující akce:

- Zadejte příkazy z aplikačního programu, který vydává příkazy PCF, nebo příkazy MQSC v rámci příkazu Escape PCF, pokud tyto příkazy nemanipulují s inicializátory kanálu. (Tyto příkazy jsou popsány v části “Ochrana definic inicializátoru kanálu” na stránce 115).

- Zadejte volání MQI z aplikačního programu (pokud nechcete použít vazby rychlé cesty pro volání MQCONNX).
- Příkaz `crtmqcvx` slouží k vytvoření fragmentu kódu, který provádí převod dat ve strukturách datových typů.
- Pomocí příkazu `dspmq` zobrazte správce front.
- Použijte příkaz `dspmqtrc` k zobrazení IBM MQ formátovaného výstupu trasování.

Omezení na 12 znaků se vztahuje jak na ID skupiny, tak na ID uživatele.

Platformy UNIX and Linux obecně omezují délku ID uživatele na 12 znaků. Produkt AIX 5.3 zvýšil tento limit, ale produkt IBM MQ nadále dodržuje omezení na 12 znaků na všech platformách UNIX and Linux . Pokud použijete ID uživatele delší než 12 znaků, IBM MQ jej nahradí hodnotou `UNKNOWN`. Nedefinujte ID uživatele s hodnotou `UNKNOWN`.

ALW Správa skupiny mqm na systému AIX, Linux, and Windows

Uživatelům ve skupině mqm jsou udělena úplná oprávnění k administraci pro produkt IBM MQ. Z tohoto důvodu byste neměli registrovat aplikace a běžné uživatele ve skupině mqm. Skupina mqm by měla obsahovat pouze účty administrátorů systému IBM MQ .

Tyto úlohy jsou popsány v:

- Windows Vytvoření a správa skupin na systému Windows
- AIX Vytvoření a správa skupin na systému AIX
- Linux Vytvoření a správa skupin na systému Linux

Windows Pokud je váš řadič domény spuštěn na systému Windows 2000 nebo Windows 2003 nebo novějším, bude možná muset administrátor domény nastavit speciální účet, který bude produkt IBM MQ používat. Další informace viz Konfigurace IBM MQ s Prepare IBM MQ Wizard a Vytvoření a nastavení Windows doménových účtů pro produkt IBM MQ.

ALW Oprávnění pro práci s objekty IBM MQ na systému AIX, Linux, and Windows

Všechny objekty jsou chráněny produktem IBM MQa činitelům musí být uděleno příslušné oprávnění pro přístup k nim. Různí činitelé potřebují různá přístupová práva k různým objektům.

Ke správcům front, frontám, definicím procesů, seznamům názvů, kanálům, kanálům připojení klienta, modulům listener, službám a objektům ověřovacích informací se přistupuje z aplikací, které používají volání MQI nebo příkazy PCF. Všechny tyto prostředky jsou chráněny produktem IBM MQa aplikacím je třeba udělit oprávnění k jejich přístupu. Entita, která vytváří požadavek, může být uživatel, aplikační program, který vydává volání MQI, nebo administrační program, který vydává příkaz PCF. Na identifikátor žadatele se odkazuje jako na *činitele*.

Různým skupinám činitelů lze udělit různé typy přístupových oprávnění ke stejnému objektu. Například pro specifickou frontu může být jedné skupině povoleno provádět operace vložení i získání; jiné skupině může být povoleno pouze procházet frontu (`MQGET` s volbou procházení). Podobně některé skupiny mohly vložit a získat oprávnění k frontě, ale neměly povoleno měnit atributy fronty nebo ji odstranit.

Některé operace jsou obzvláště citlivé a měly by být omezeny na privilegované uživatele. Příklad:

- Přístup k některým speciálním frontám, jako jsou přenosové fronty nebo fronta příkazů SYSTEM.ADMIN.COMMAND.QUEUE
- Spuštění programů, které používají úplné volby kontextu MQI
- Vytvoření a odstranění front aplikací

Úplná přístupová oprávnění k objektu jsou automaticky udělena ID uživatele, který objekt vytvořil, a všem členům skupiny mqm (a členům skupiny lokálních administrátorů v systémech Windows).

Související pojmy

"Oprávnění ke správě IBM MQ v systému AIX, Linux, and Windows" na stránce 419
Administrátoři produktu IBM MQ mohou použít všechny příkazy produktu IBM MQ a udělit oprávnění ostatním uživatelům. Když administrátoři zadávají příkazy pro vzdálené správce front, musí mít požadované oprávnění pro vzdáleného správce front. Další aspekty platí pro systémy Windows .

ALW Při provádění kontrol zabezpečení na systému AIX, Linux, and Windows

Kontroly zabezpečení se obvykle provádějí při připojování ke správci front, otevírání nebo zavírání objektů a vkládání nebo získávání zpráv.

Bezpečnostní kontroly provedené pro typickou aplikaci jsou následující:

Připojení ke správci front (volání MQCONN nebo MQCONNX)
Jedná se o první přidružení aplikace ke konkrétnímu správci front. Správce front zjišťuje provozní prostředí a zjišťuje ID uživatele přidružené k aplikaci. Produkt IBM MQ poté ověří, zda je ID uživatele autorizováno pro připojení ke správci front, a uchová ID uživatele pro budoucí kontroly.

Uživatelé se nemusí přihlašovat k produktu IBM MQ; produkt IBM MQ předpokládá, že se uživatelé přihlásili k základnímu operačnímu systému a byli tímto ověřeni.

Otevření objektu (volání MQOPEN nebo MQPUT1)
K objektům produktu IBM MQ se přistupuje otevřením objektu a zadáním příkazů pro tento objekt. Všechny kontroly prostředků se provádějí při otevření objektu, nikoli při skutečnému přístupu k objektu. To znamená, že požadavek **MQOPEN** musí uvádět požadovaný typ přístupu (například, zda chce uživatel pouze procházet objekt nebo provést aktualizaci, jako je vložení zpráv do fronty).

Produkt IBM MQ zkontroluje prostředek, který je uveden v požadavku **MQOPEN** . Pro alias nebo objekt vzdálené fronty se používá autorizace objektu samotného, nikoli fronty, do které se alias nebo vzdálená fronta převádí. To znamená, že uživatel nepotřebuje oprávnění pro přístup k němu. Omezte oprávnění k vytváření front na oprávněné uživatele. Pokud tak neučiníte, uživatelé mohou obejít běžné řízení přístupu jednoduše vytvořením aliasu. Pokud se na vzdálenou frontu odkazuje explicitně s názvem fronty i názvem správce front, zkontroluje se přenosová fronta přidružená ke vzdálenému správci front.

Oprávnění k dynamické frontě je založeno na oprávnění modelové fronty, ze které je odvozeno, ale nemusí být nutně stejné. To je popsáno v poznámce "1" na stránce 134.

ID uživatele používané správcem front pro kontroly přístupu je ID uživatele získané z provozního prostředí aplikace připojené ke správci front. Vhodně autorizovaná aplikace může vydat volání **MQOPEN** uvádějící alternativní ID uživatele; kontroly řízení přístupu se pak provádějí na alternativním ID uživatele. Tím se nezmění ID uživatele přidružené k aplikaci, které se používá pouze pro kontroly řízení přístupu.

Vkládání a získávání zpráv (volání MQPUT nebo MQGET)
Neprovádějí se žádné kontroly řízení přístupu.

Zavření objektu (MQCLOSE)
Neprovádějí se žádné kontroly řízení přístupu, pokud **MQCLOSE** nezpůsobí odstranění dynamické fronty. V tomto případě existuje kontrola, zda je ID uživatele autorizováno k odstranění fronty.

Přihlášení k odběru tématu (MQSUB)
Když se aplikace přihlásí k odběru tématu, uvádí typ operace, kterou musí provést. Buďto vytváří nový odběr, mění existující odběr, nebo obnovuje existující odběr beze změny. Pro každý typ operace správce front kontroluje, zda má ID uživatele přidružené k aplikaci oprávnění k provedení operace.

Když se aplikace přihlásí k odběru tématu, jsou provedeny kontroly oprávnění pro objekty tématu, které se nacházejí ve stromu témat ve stromu témat nebo nad bodem ve stromu témat, k jehož odběru se aplikace přihlásí. Kontroly oprávnění mohou zahrnovat kontroly více než jednoho objektu tématu.

ID uživatele, které správce front používá pro kontroly oprávnění, je ID uživatele získané z operačního systému při připojení aplikace ke správci front.

Správce front provádí kontroly oprávnění ve frontách odběratelů, nikoli však ve spravovaných frontách.

ALW Jak je řízení přístupu implementováno produktem IBM MQ on AIX, Linux, and Windows

Produkt IBM MQ používá služby zabezpečení poskytované základním operačním systémem pomocí správce oprávnění k objektu. Produkt IBM MQ poskytuje příkazy pro vytváření a údržbu seznamů přístupových práv.

Rozhraní řízení přístupu s názvem rozhraní služby autorizace je součástí produktu IBM MQ. Produkt IBM MQ dodává implementaci správce řízení přístupu (v souladu s rozhraním služby autorizace) známého jako *správce oprávnění k objektu (OAM)*. Tato volba je automaticky instalována a povolena pro každého vytvořeného správce front, není-li uvedeno jinak (jak je popsáno v tématu “Zabránění kontrolám zabezpečených přístupů na systémech AIX, Linux, and Windows” na stránce 382). Komponenta OAM může být nahrazena libovolnou komponentou napsanou uživatelem nebo dodavatelem, která je v souladu s rozhraním služby autorizace.

OAM využívá funkce zabezpečení základního operačního systému pomocí ID uživatelů a skupin operačního systému. Uživatelé mohou k objektům produktu IBM MQ přistupovat pouze v případě, že mají správné oprávnění. “Řízení přístupu k objektům pomocí OAM na systému AIX, Linux, and Windows” na stránce 372 popisuje, jak udělit a odvolat toto oprávnění.

OAM udržuje seznam přístupových práv (ACL) pro každý prostředek, který řídí. Data autorizace jsou uložena v lokální frontě s názvem SYSTEM.AUTH.DATA.QUEUE. Přístup k této frontě je omezen na uživatele ve skupině mqm, a dále na uživatele v systému Windows, na uživatele ve skupině Administrátoři a na uživatele přihlášené pomocí ID systému. Uživatelský přístup k frontě nelze změnit.

Produkt IBM MQ poskytuje příkazy pro vytváření a údržbu seznamů přístupových práv. Další informace o těchto příkazech viz “Řízení přístupu k objektům pomocí OAM na systému AIX, Linux, and Windows” na stránce 372.

Produkt IBM MQ předá OAM požadavek obsahující činitele, název prostředku a typ přístupu. Modul OAM uděluje nebo zamítá přístup na základě seznamu ACL, který udržuje. IBM MQ následuje po rozhodnutí OAM; pokud OAM nemůže učinit rozhodnutí, IBM MQ nepovolí přístup.

ALW Identifikace ID uživatele v systému AIX, Linux, and Windows

Správce oprávnění k objektu identifikuje činitele, který požaduje přístup k prostředku. ID uživatele použité jako činitel se liší v závislosti na kontextu.

Správce oprávnění k objektu (OAM) musí být schopen identifikovat, kdo požaduje přístup ke konkrétnímu prostředku. Produkt IBM MQ používá k odkazování na tento identifikátor výraz *činitel* . Činitel je vytvořen při prvním připojení aplikace ke správci front; je určen správcem front z ID uživatele přidruženého k připojující se aplikaci. (Pokud aplikace zadá volání XA bez připojení ke správci front, bude ID uživatele přidružené k aplikaci, která vydává volání xa_open, použito pro kontroly oprávnění správcem front.)

V systémech AIX and Linux autorizační rutiny kontrolujou buď skutečné (přihlášené) ID uživatele, nebo efektivní ID uživatele přidružené k aplikaci. Kontrolované ID uživatele může být závislé na typu vazby, podrobnosti viz Instalovatelné služby.

Produkt IBM MQ šíří ID uživatele přijaté ze systému v záhlaví zprávy (struktura MQMD) každé zprávy jako identifikaci uživatele. Tento identifikátor je součástí informací o kontextu zprávy a je popsán v části “Kontextové oprávnění na systému AIX, Linux, and Windows” na stránce 426. Aplikace nemohou tyto informace měnit, pokud nebyly autorizovány ke změně informací o kontextu.

ALW *Činitelé a skupiny na AIX, Linux, and Windows*

Činitelé mohou patřit do skupin. Udělíte-li přístup k prostředkům skupinám a nikoli jednotlivcům, můžete snížit požadovaný objem administrace. Seznamy přístupových práv (ACL) jsou založeny na skupinách i ID uživatelů.

Můžete například definovat skupinu sestávající z uživatelů, kteří chtějí spustit konkrétní aplikaci. Ostatním uživatelům může být udělen přístup ke všem prostředkům, které vyžadují, přidáním jejich ID uživatele do příslušné skupiny.

Tento proces definování a správy skupin je popsán pro konkrétní platformy:

- AIX Vytvoření a správa skupin na systému AIX
- Linux Vytvoření a správa skupin na systému Linux
- Windows Vytvoření a správa skupin na systému Windows

Činitel může patřit do více než jedné skupiny (její sada skupin). Má souhrn všech oprávnění udělených každé skupině ve své skupině. Tato oprávnění jsou uložena v mezipaměti, takže veškeré změny provedené v členství činitele ve skupině budou rozpoznány až po restartování správce front, pokud nezadáte příkaz MQSC **REFRESH SECURITY** (nebo jeho ekvivalent PCF).

Linux AIX Systémy AIX and Linux

V systému IBM MQ 8.0jsou seznamy přístupových práv (ACL) založeny jak na ID uživatelů, tak na skupinách a můžete je použít pro autorizaci nastavením atributu **SecurityPolicy** na odpovídající hodnotu, jak je popsáno v části Sekce služby souboru qm.ini a Konfigurace sekcí autorizační služby na systému AIX and Linux.

V produktu IBM MQ 8.0můžete pro autorizaci použít *model založený na uživateli* , což vám umožňuje používat uživatele i skupiny. Určíte-li však uživatele v příkazu setmqaut , budou nová oprávnění platit pouze pro tohoto uživatele a nikoli pro žádné skupiny, do kterých tento uživatel patří. Další informace viz “Oprávnění založená na uživateli OAM na AIX and Linux” na stránce 373.

Při použití *modelu založeného na skupině* pro autorizaci je primární skupina, do které patří ID uživatele, zahrnuta v seznamu přístupových práv. Individuální ID uživatele není zahrnuto a oprávnění je uděleno všem členům této skupiny. Z tohoto důvodu si uvědomte, že můžete neúmyslně změnit oprávnění činitele změnou oprávnění jiného činitele ve stejné skupině.

Všichni uživatelé jsou nominálně přiřazeni k výchozí skupině uživatelů `nikdo` a standardně nejsou této skupině udělovány žádné autorizace. Můžete změnit autorizaci ve skupině `nikdo` , chcete-li udělit přístup k prostředkům IBM MQ uživatelům bez specifických autorizací.

V 9.3.0 Od IBM MQ 9.3.0můžete použít volbu `UserExternal` atributu **SecurityPolicy** k vytvoření jména uživatele jiného než operačního systému. Pokud vytvoříte jméno uživatele jiného než operačního systému, bude tento uživatel považován za uživatele, který nepatří do žádné skupiny, kromě skupiny nobody . Další informace o této volbě viz crtmqm a Sekce služby souboru qm.ini.

Nedefinujte ID uživatele s hodnotou `UNKNOWN`. Hodnota `UNKNOWN` se používá, když je ID uživatele příliš dlouhé, takže libovolná ID uživatele by použila přístupová oprávnění `UNKNOWN`.

Informace o použití LDAP naleznete v části “Nastavení autorizací” na stránce 432 .

ID uživatelů mohou obsahovat až 12 znaků a názvy skupin až 12 znaků.

Windows Systémy Windows

Seznamy ACL jsou založeny jak na ID uživatelů, tak na skupinách. Kontroly jsou stejné jako pro AIX and Linux. Můžete mít různé uživatele na různých doménách se stejným ID uživatele. Produkt IBM MQ umožňuje, aby ID uživatelů byla kvalifikována pomocí názvu domény, takže těmto uživatelům mohou být uděleny různé úrovně přístupu.

Název skupiny může volitelně obsahovat název domény určený v následujících formátech:

```
GroupName@domain domain_name\group_name
```

Globální skupiny jsou OAM kontrolovány pouze ve dvou případech:

1. Sekce zabezpečení správce front obsahuje nastavení: `GroupModel=GlobalGroups`. Viz Zabezpečení.

2. Správce front používá alternativní skupinu zabezpečeného přístupu. Viz **crtmqm** .

ID uživatelů mohou obsahovat až 20 znaků, názvy domén až 15 znaků a názvy skupin až 64 znaků.

Modul OAM nejprve zkontroluje lokální databázi zabezpečení, poté databázi primární domény a nakonec databázi všech důvěryhodných domén. První nalezené ID uživatele je používáno modulem OAM pro kontrolu. Každé z těchto ID uživatelů může mít různá členství ve skupinách na konkrétním počítači.

Některé řídicí příkazy (například **crtmqm**) mění oprávnění na objektech IBM MQ pomocí správce OAM (Object Authority Manager). OAM prohledává databáze zabezpečení v pořadí uvedeném v předchozím odstavci, aby určil oprávnění pro konkrétní ID uživatele. V důsledku toho může oprávnění určené modulem OAM přepsat skutečnost, že ID uživatele je členem lokální skupiny mqm. Pokud například zadáte příkaz **crtmqm** z ID uživatele ověřeného řadičem domény, který má členství v lokální skupině mqm prostřednictvím globální skupiny, příkaz se nezdaří, pokud má systém lokálního uživatele se stejným názvem, který není v lokální skupině mqm.

Další informace o nastavení atributu **SecurityPolicy** v systému Windowsnaleznete v tématech Instalovatelné služby a Konfigurace sekcí autorizační služby v systému Windows.

Windows *Identifikátory zabezpečení Windows (SID)*

IBM MQ on Windows používá SID, kde je k dispozici. Pokud není Windows SID dodán s požadavkem na autorizaci, IBM MQ identifikuje uživatele na základě samotného jména uživatele, ale to může vést k udělení nesprávného oprávnění.

V systémech Windows se identifikátor zabezpečení (SID) používá k doplnění ID uživatele. Identifikátor SID obsahuje informace, které identifikují úplné podrobnosti o uživatelském účtu v databázi správce SAM (security account manager) produktu Windows , kde je uživatel definován. Když je v systému IBM MQ for Windowsvytvořena zpráva, produkt IBM MQ uloží identifikátor SID do deskriptoru zprávy. Když IBM MQ on Windows provádí kontroly autorizace, používá identifikátor SID k dotazování na úplné informace z databáze SAM. (Databáze SAM, ve které je uživatel definován, musí být přístupná, aby byl tento dotaz úspěšný.)

Standardně, pokud není Windows SID dodáno s požadavkem na autorizaci, IBM MQ identifikuje uživatele na základě samotného jména uživatele. To se provádí prohledáváním databází zabezpečení v následujícím pořadí:

1. Lokální databáze zabezpečení
2. Databáze zabezpečení primární domény
3. Databáze zabezpečení důvěryhodných domén

Není-li jméno uživatele jedinečné, může být uděleno nesprávné oprávnění IBM MQ . Chcete-li tomuto problému zabránit, zahrňte identifikátor SID do každého požadavku na autorizaci; identifikátor SID používá produkt IBM MQ k zavedení pověření uživatele.

Chcete-li uvést, že všechny požadavky na autorizaci musí obsahovat SID, použijte **regedit**. Nastavte SecurityPolicy na hodnotu NTSIDsRequired.

ALW Oprávnění alternativního uživatele na systému AIX, Linux, and Windows

Můžete uvést, že ID uživatele může použít oprávnění jiného uživatele při přístupu k objektu IBM MQ . Toto se nazývá *oprávnění alternativního uživatele*a můžete jej použít na libovolném objektu IBM MQ .

Oprávnění alternativního uživatele je nezbytné v případech, kdy server přijímá požadavky od programu a chce se ujistit, že program má požadované oprávnění k požadavku. Server může mít požadované oprávnění, ale musí vědět, zda má program oprávnění pro akce, které požadoval.

Předpokládejme například, že program serveru spuštěný pod ID uživatele PAYSERV načte zprávu požadavku z fronty, která byla vložena do fronty podle ID uživatele USER1. Když program serveru obdrží zprávu požadavku, zpracuje požadavek a vloží odpověď zpět do fronty pro odpověď uvedené se zprávou požadavku. Místo použití vlastního ID uživatele (PAYSERV) k autorizaci otevření fronty pro odpověď

může server zadat jiné ID uživatele, v tomto případě USER1. V tomto příkladu můžete použít oprávnění alternativního uživatele k řízení, zda je PAYSERV oprávněn uvést USER1 jako alternativní ID uživatele, když otevře frontu pro odpověď.

ID alternativního uživatele je uvedeno v poli **AlternateUserId** deskriptoru objektu.

Linux Řešení určitých problémů s členstvím ve skupinách na Linux

Některé systémy pomalu vracejí informace o skupinách prostřednictvím běžné řady volání rozhraní API operačního systému **getgrent** , a pokud má váš podnik tisíce skupin k vyhledávání a hledá skupiny, ve kterých se uživatel produktu mqm nachází, může tato pomalá odezva způsobit vypršení časového limitu interního správce front. Chcete-li tento problém obejít, existuje alternativní rozhraní API operačního systému.

Chcete-li použít alternativní rozhraní API, které je rychlejší, a vrátit všechny skupiny z jednoho volání, nastavte proměnnou prostředí MQS_GETGROUPLIST_API.

Možná jste obdrželi chybu RC2035 při udělování přístupu pro připojení k sekundární skupině uživatele a povolení proměnné MQS_GETGROUPLIST_API zmírňuje problém.

Produkt IBM MQ pak použije rozhraní API **getgrouplist** namísto rozhraní API **getgrent** .

Chcete-li povolit **getgrouplist**:

1. Zastavit správce front
2. Zadejte příkaz export MQS_GETGROUPLIST_API=1
3. Restartovat správce front

Zopakujte scénář, který se nezdařil, a pokud byl problém vyřešen, můžete zvážit úpravu souboru .bashrc / .profile pro uživatele mqm , abyste přidali tuto proměnnou prostředí, nebo přidejte proměnnou prostředí do skriptu, který používáte ke spuštění správce front.

Pokud váš systém sloučí informace o uživatelích nebo skupinách operačního systému z více úložišť, jako je NIS nebo LDAP, pak se ujistěte, že skupina nebo ID uživatele jsou konzistentní ve všech úložištích včetně lokálního, protože se používají k instalaci a nastavení oprávnění na úrovni operačního systému.

ALW Kontextové oprávnění na systému AIX, Linux, and Windows

Kontext je informace, která se týká konkrétní zprávy a je obsažena v deskriptoru zprávy MQMD, který je součástí zprávy. Aplikace mohou určit data kontextu při volání MQOPEN nebo MQPUT .

Informace o kontextu jsou k dispozici ve dvou sekcích:

Sekce identity
Kdo ten vzkaz přišel. Skládá se z polí UserIdentifier, AccountingTokena ApplIdentityData .

Oddíl původu
Odkud zpráva přišla a kdy byla vložena do fronty. Skládá se z polí PutApplType, PutApplName, PutDate, PutTimea ApplOriginData .

Aplikace mohou určit data kontextu při volání MQOPEN nebo MQPUT . Tato data mohou být generována aplikací, předána z jiné zprávy nebo standardně generována správcem front. Například, data kontextu mohou být použita programy serveru ke kontrole identity žadatele, testování, zda zpráva pochází z aplikace spuštěné pod ID autorizovaného uživatele.

Program serveru může použít UserIdentifier k určení ID uživatele alternativního uživatele. Pomocí autorizace kontextu můžete určit, zda může uživatel zadat libovolnou z voleb kontextu pro libovolné volání MQOPEN nebo MQPUT1 .

Viz Informace o řízení kontextu , kde získáte informace o volbách kontextu, a MQMD-Deskriptor zpráv , kde najdete popisy polí deskriptoru zpráv souvisejících s kontextem.

Implementace řízení přístupu v uživatelských procedur zabezpečení

Řízení přístupu můžete implementovat v uživatelské proceduře zabezpečení pomocí MCAUserIdentifier nebo správce oprávnění k objektu.

MCAUserIdentifier

Každá aktuální instance kanálu má přidruženou strukturu definice kanálu MQCD. Počáteční hodnoty polí v MQCD jsou určeny definicí kanálu vytvořenou administrátorem produktu IBM MQ . Zejména počáteční hodnota jednoho z polí, *MCAUserIdentifier*, je určena hodnotou parametru MCAUSER v příkazu DEFINE CHANNEL nebo ekvivalentem hodnoty MCAUSER, pokud je definice kanálu vytvořena jiným způsobem.

Struktura MQCD je předána programu uživatelské procedury kanálu, je-li volána agentem MCA. Je-li uživatelská procedura zabezpečení volána agentem MCA, může uživatelská procedura zabezpečení změnit hodnotu parametru *MCAUserIdentifier*a nahradit libovolnou hodnotu určenou v definici kanálu.

Multi Pokud v systému Multiplatformsnení hodnota *MCAUserIdentifier* prázdná, správce front použije hodnotu *MCAUserIdentifier* jako ID uživatele pro kontrolu oprávnění, když se MCA pokusí získat přístup k prostředkům správce front poté, co se připojí ke správci front. Je-li hodnota *MCAUserIdentifier* prázdná, použije správce front místo toho výchozí ID uživatele MCA. To platí pro kanály RCVR, RQSTR, CLUSRCVR a SVRCONN. Pro odesílání MCA se vždy použije výchozí ID uživatele pro kontroly oprávnění, i když hodnota *MCAUserIdentifier* není prázdná.

z/OS V systému z/OSmůže správce front použít hodnotu *MCAUserIdentifier* pro kontroly oprávnění, pokud není prázdná. Pro příjem MCA a MCA připojení serveru závisí to, zda správce front používá hodnotu *MCAUserIdentifier* pro kontroly oprávnění, na:

- Hodnota parametru PUTAUT v definici kanálu
- Profil RACF použitý pro kontroly
- Úroveň přístupu ID uživatele adresního prostoru inicializátoru kanálu k profilu RESLEVEL

Pro odesílání MCA to závisí na:

- Zda odesílající agent MCA je volající nebo odpovídací modul
- Úroveň přístupu ID uživatele adresního prostoru inicializátoru kanálu k profilu RESLEVEL

ID uživatele, které uživatelská procedura zabezpečení ukládá do *MCAUserIdentifier* , lze získat různými způsoby. Několik příkladů:

- V případě, že na konci klienta kanálu MQI neexistuje žádná uživatelská procedura zabezpečení, přechází ID uživatele přidružené k aplikaci klienta IBM MQ z agenta MCA připojení klienta do agenta MCA připojení serveru, když aplikace klienta zadá volání MQCONN.Agent MCA připojení serveru ukládá toto ID uživatele do pole *RemoteUser* ve struktuře definice kanálu MQCD. Pokud je hodnota *MCAUserIdentifier* v tuto chvíli prázdná, uloží agent MCA stejné ID uživatele do *MCAUserIdentifier*. Pokud agent MCA neukládá ID uživatele do *MCAUserIdentifier*, může to uživatelská procedura zabezpečení provést později nastavením *MCAUserIdentifier* na hodnotu *RemoteUserIdentifier*.

  Pokud ID uživatele, které teče z klientského systému, vstupuje do nové domény zabezpečení a není platné v systému serveru, může uživatelská procedura zabezpečení nahradit ID uživatele, které je platné, a uložit nahrazené ID uživatele do *MCAUserIdentifier*.
- ID uživatele může být odesláno uživatelskou procedurou zabezpečení partnera ve zprávě zabezpečení.

  V kanálu zpráv může uživatelská procedura zabezpečení volaná odesílajícím agentem MCA odeslat ID uživatele, pod kterým je odesílající agent MCA spuštěn. Uživatelská procedura zabezpečení volaná přijímajícím agentem MCA pak může uložit ID uživatele do *MCAUserIdentifier*. Podobně v kanálu MQI může uživatelská procedura zabezpečení na straně klienta kanálu odeslat ID uživatele přidružené k aplikaci IBM MQ MQI client . Uživatelská procedura zabezpečení na konci serveru kanálu pak může uložit ID uživatele do *MCAUserIdentifier*. Stejně jako v předchozím příkladu, pokud ID uživatele není v cílovém systému platné, může uživatelská procedura zabezpečení nahradit ID uživatele, které je platné, a uložit nahrazené ID uživatele v *MCAUserIdentifier*.

Pokud je digitální certifikát přijat jako součást identifikační a ověřovací služby, může uživatelská procedura zabezpečení mapovat rozlišující název v certifikátu na ID uživatele, které je platné na cílovém systému. Poté může uložit ID uživatele do *MCAUserIdentifier*.

- Pokud je v kanálu použito zabezpečení TLS, rozlišující název (DN) partnera je předán uživatelské proceduře v poli Ptr SSLPeerNameMQCD a rozlišující název vydavatele tohoto certifikátu je předán uživatelské proceduře v poli SSLRemCertIssNamePtr MQCXP.

Další informace o poli *MCAUserIdentifier* , struktuře definice kanálu MQCD a struktuře parametrů uživatelské procedury kanálu MQCXP naleznete v tématu Volání a datové struktury uživatelské procedury kanálu. Další informace o ID uživatele, které pochází ze systému klienta v kanálu MQI, naleznete v tématu Řízení přístupu.

Poznámka: Aplikace uživatelské procedury zabezpečení vytvořené před vydáním produktu IBM WebSphere MQ 7.1 mohou vyžadovat aktualizaci. Další informace naleznete v tématu Programy uživatelských procedur pro zabezpečení kanálu.

Ověření uživatele správce oprávnění k objektu IBM MQ

V připojeních systému IBM MQ MQI client lze uživatelské procedury zabezpečení použít k úpravě nebo vytvoření struktury MQCSP používané v ověřování uživatelů OAM (Object Authority Manager). To je popsáno v tématu Programy uživatelské procedury kanálu pro kanály systému zpráv .

Implementace řízení přístupu v uživatelských procedur pro zprávy

Možná budete muset použít uživatelskou proceduru pro zprávu, abyste nahradili jedno ID uživatele jiným.

Zvažte aplikaci klienta, která odešle zprávu serverové aplikaci. Serverová aplikace může extrahovat ID uživatele z pole *UserIdentifier* v deskriptoru zprávy a za předpokladu, že má alternativní oprávnění uživatele, požádat správce front o použití tohoto ID uživatele pro kontrolu oprávnění při přístupu k prostředkům produktu IBM MQ jménem klienta.

Pokud je parametr PUTAUT nastaven na CTX (nebo ALTMCA na z/OS) v definici kanálu se ID uživatele v poli *UserIdentifier* každé příchozí zprávy použije pro kontrolu oprávnění, když MCA otevře cílovou frontu.

Za určitých okolností, když je zpráva sestavy generována, je vložena pomocí oprávnění ID uživatele v poli *UserIdentifier* zprávy, která způsobuje sestavu. S tímto oprávněním jsou vždy předkládány zejména zprávy o potvrzení při doručení (COD) a zprávy o vypršení platnosti.

Kvůli těmto situacím může být nezbytné nahradit jedno ID uživatele jiným ID v poli *UserIdentifier* , když zpráva vstupuje do nové domény zabezpečení. To lze provést pomocí uživatelské procedury pro zprávy na přijímacím konci kanálu. Případně se můžete ujistit, že ID uživatele v poli *UserIdentifier* příchozí zprávy je definováno v nové doméně zabezpečení.

Pokud příchozí zpráva obsahuje digitální certifikát pro uživatele aplikace, která zprávu odeslala, může uživatelská procedura zprávy ověřit certifikát a namapovat rozlišující název v certifikátu na ID uživatele, které je platné v přijímajícím systému. Pak může nastavit pole *UserIdentifier* v deskriptoru zprávy na toto ID uživatele.

Je-li nezbytné, aby uživatelská procedura pro zprávy změnila hodnotu pole *UserIdentifier* v příchozí zprávě, může být vhodné, aby uživatelská procedura pro zprávy současně ověřila odesilatele zprávy. Další informace naleznete v tématu “Mapování identit v uživatelských procedur zpráv” na stránce 347.

Implementace řízení přístupu v uživatelské proceduře rozhraní API a uživatelské proceduře rozhraní API

Rozhraní API nebo uživatelská procedura přechodu rozhraní API může poskytnout řízení přístupu k doplnění řízení přístupu poskytovaných produktem IBM MQ. Uživatelská procedura může zejména poskytovat řízení přístupu na úrovni zpráv. Uživatelská procedura může zajistit, že aplikace vloží do fronty nebo získá z fronty pouze ty zprávy, které splňují určitá kritéria.

Zvažte následující příklady:

- Zpráva obsahuje informace o objednávce. Když se aplikace pokusí vložit zprávu do fronty, může rozhraní API nebo uživatelská procedura přechodu rozhraní API zkontrolovat, zda je celková hodnota objednávky menší než předepsaný limit.
- Zprávy přicházejí do cílové fronty od vzdálených správců front. Když se aplikace pokusí získat zprávu z fronty, může rozhraní API nebo uživatelská procedura přechodu rozhraní API zkontrolovat, zda je odesilatel zprávy oprávněn odeslat zprávu do fronty.

Multi V 9.3.0 Zabezpečení kontinuálních front

Funkce proudových front umožňuje administrátorovi konfigurovat lokální (nebo modelovou) frontu se sekundární frontou, kde jsou umístěny duplicitní zprávy, kdykoli je zpráva vložena do původní fronty. Existují dva aspekty, které je třeba zvážit, pokud jde o oprávnění pro streamování front.

Oprávnění ke konfiguraci fronty pro streamování duplicitních zpráv

Chcete-li povolit streamování duplicitních zpráv z jedné fronty do sekundární fronty, musíte k tomu mít oprávnění. Oprávnění ke konfiguraci atributu **STREAMQ** fronty vyžaduje následující oprávnění:

1. Oprávnění CSDB fronty, pro kterou mění atribut **STREAMQ**
2. Oprávnění CSDB fronty, do které mají být vloženy zprávy duplikace

Kombinace těchto dvou kontrol oprávnění v době konfigurace zajišťuje, že uživatel, který má pouze oprávnění CHG v původní frontě, nemůže způsobit vložení zpráv do jiné fronty, pro kterou nemá žádná oprávnění.

Oprávnění k otevření fronty nebo front a vložení zpráv

Když aplikace otevře frontu, která byla konfigurována se sekundární frontou, prostřednictvím svého atributu **STREAMQ** se provede kontrola oprávnění, že uživatel aplikace má oprávnění PUT na původní frontě.

Poznámka: Pro uživatele aplikace v sekundární frontě není provedena žádná další kontrola oprávnění, která je podobná modelu oprávnění použitému pro alias fronty.

Aplikace, které spotřebovávají zprávy z původní nebo sekundární fronty, vyžadují oprávnění GET nebo BROWSE pouze ve frontě, ze které spotřebovávají.

Při vložení nebo získání času se neprovádějí žádné další kontroly oprávnění.

Příklad

V následujícím příkladu jsou uvedena správná oprávnění, která jsou nastavena tak, aby uživateli `admin` umožnila konfigurovat původní frontu INQUIRIES.QUEUE, chcete-li vysílat duplicitní zprávy do lokální fronty ANALYTICS.QUEUE, ale zabraňuje produktu `admin` duplikovat zprávy do PURCHASES.QUEUE:

```
SET AUTHREC PROFILE(INQUIRIES.QUEUE) PRINCIPAL('admin') AUTHADD(CHG)
SET AUTHREC PROFILE(ANALYTICS.QUEUE) PRINCIPAL('admin') AUTHADD(CHG)
SET AUTHREC PROFILE(PURCHASES.QUEUE) PRINCIPAL('admin') AUTHRMV(CHG)
```

Uživatel `admin` pak může zadat následující příkaz:

```
ALTER QLOCAL(INQUIRIES.QUEUE) STREAMQ(ANALYTICS.QUEUE)
```

ale pokud stejný uživatel zadá následující příkaz:

```
ALTER QLOCAL(INQUIRIES.QUEUE) STREAMQ(PURCHASES.QUEUE)
```

chcete-li konfigurovat INQUIRIES.QUEUE pro vložení duplicitních zpráv do PURCHASES.QUEUE, obdrží následující chybu:

```
AMQ8135E Neautorizováno
```

S INQUIRIES.QUEUE nakonfigurovaná tak, aby duplikovala zprávy do produktu ANALYTICS.QUEUE, následující záznamy oprávnění se používají k tomu, aby umožnily aplikaci spuštěné jako uživatel `appuser` vkládat zprávy do INQUIRIES.QUEUEa duplicitní zprávy pro ANALYTICS.QUEUE:

```
SET AUTHREC PROFILE(INQUIRIES.QUEUE) PRINCIPAL('appuser') AUTHADD(PUT)
```

Poznámka: Produkt `appuser` nevyžaduje záznam oprávnění v produktu ANALYTICS.QUEUE. Správce front vloží do fronty duplicitní zprávy.

Související pojmy
Fronty proudu

V 9.3.0 z/OS Zabezpečení datových proudů front v systému z/OS

Funkce proudových front umožňuje administrátorovi konfigurovat lokální (nebo modelovou) frontu se sekundární frontou, kde jsou umístěny duplicitní zprávy, kdykoli je zpráva vložena do původní fronty. Existují dva aspekty, které je třeba zvážit, pokud jde o oprávnění pro streamování front.

Oprávnění ke konfiguraci fronty pro streamování duplicitních zpráv

Chcete-li povolit streamování duplicitních zpráv z jedné fronty do sekundární fronty, musíte k tomu mít oprávnění. Oprávnění ke konfiguraci atributu **STREAMQ** fronty vyžaduje, abyste měli následující nastavení profilů:

1. ALTER pro úroveň přístupu k MQADMIN nebo MXADMIN pro frontu, pro kterou mění atribut **STREAMQ**
2. ALTER pro úroveň přístupu k MQADMIN nebo MXADMIN pro frontu, do které chcete vysílat zprávy

Kombinace těchto kontrol zabezpečení v době konfigurace zajišťuje, že uživatel, který má pouze přístup ALTER k původní frontě, nemůže způsobit vložení zpráv do jiné fronty, pro kterou nemá žádná oprávnění.

Oprávnění k otevření fronty nebo front a vložení zpráv

Když aplikace otevře frontu, která byla konfigurována se sekundární frontou, prostřednictvím jejího atributu **STREAMQ** se provede kontrola oprávnění, že uživatel aplikace má oprávnění UPDATE k původní frontě.

Poznámka: Pro uživatele aplikace v sekundární frontě není provedena žádná další kontrola oprávnění, která je podobná modelu oprávnění použitému pro alias fronty.

Aplikace, které spotřebovávají zprávy z původní nebo sekundární fronty, vyžadují oprávnění UPDATE nebo READ, pouze ve frontě, ze které spotřebovávají.

Při vložení nebo získání času se neprovádějí žádné další kontroly oprávnění.

Příklad

V následujícím příkladu jsou uvedeny správné profily, které jsou nastaveny tak, aby uživateli `ADMIN` umožnily konfigurovat původní frontu INQUIRIES.QUEUE, pro streamování zpráv do lokální fronty ANALYTICS.QUEUE pomocí RACF:

```
RDEFINE MQCMDS <QMGR>.ALTER.QLOCAL UACC(NONE) OWNER(<OWNER>)
PERMIT <QMGR>.ALTER.QLOCAL CLASS(MQCMDS) ID(ADMIN) ACCESS(ALTER)

RDEFINE MQADMIN <QMGR>.QUEUE.INQUIRIES.QUEUE UACC(NONE) OWNER(<OWNER>)
PERMIT <QMGR>.QUEUE.INQUIRIES.QUEUE CLASS(MQADMIN) ID(ADMIN) ACCESS(ALTER)

RDEFINE MQADMIN <QMGR>.QUEUE.ANALYTICS.QUEUE UACC(NONE) OWNER(<OWNER>)
PERMIT <QMGR>.QUEUE.ANALYTICS.QUEUE CLASS(MQADMIN) ID(ADMIN) ACCESS(ALTER)
```

Uživatel `ADMIN` pak může zadat následující příkaz:

```
ALTER QLOCAL(INQUIRIES.QUEUE) STREAMQ(ANALYTICS.QUEUE)
```

ale pokud stejný uživatel zadá následující příkaz bez nastavení správných profilů zabezpečení:

```
ALTER QLOCAL(INQUIRIES.QUEUE) STREAMQ(PURCHASES.QUEUE)
```

chcete-li konfigurovat INQUIRIES.QUEUE pro vložení duplicitních zpráv do PURCHASES.QUEUE, obdrží následující chybu:

CSQM166I <*QMGR*> CSQMAQLC QLOCAL (*INQUIRIES.QUEUE*) NENÍ AUTORIZOVÁNA

Související pojmy

Fronty proudu

Multi Autorizace LDAP

Můžete použít autorizaci LDAP k odebrání potřeby lokálního ID uživatele.

Dostupnost autorizace LDAP na podporovaných platformách

Autorizace LDAP je k dispozici na platformě Multiplatforms:

Upozornění:

Z obecné dostupnosti produktu IBM MQ 9.0 je tato funkce k dispozici pro všechny správce front, ať už nové, nebo migrované z dřívější verze.

Přehled autorizace LDAP

Pomocí autorizace LDAP mohou příkazy, které obsluhují konfiguraci autorizace, jako např. **setmqaut** a **DISPLAY AUTHREC**, zpracovávat rozlišující názvy. Dříve byli uživatelé ověřeni porovnáním svých pověření s maximálním počtem dostupných znaků, které existují pro uživatele a skupiny v lokálním operačním systému.

Upozornění: Pokud jste spustili příkaz **DEFINE AUTHINFO** , musíte restartovat správce front. Pokud nerestartujete správce front, příkaz setmqaut nevrátí správný výsledek.

Pokud uživatel zadá ID uživatele namísto rozlišujícího názvu, bude ID uživatele zpracováno. Pokud například v kanálu s parametrem PUTAUT (CTX) existuje příchozí zpráva, znaky v ID uživatele jsou mapovány na rozlišující název LDAP a jsou provedeny příslušné kontroly autorizace.

Ostatní příkazy, jako např. **DISPLAY CONN**, pokračují v práci a zobrazují skutečnou hodnotu pro ID uživatele, i když toto ID uživatele nemusí ve skutečnosti na lokálním operačním systému existovat.

Linux AIX Při použití autorizace LDAP používá správce front vždy uživatelský model zabezpečení na platformách AIX and Linux bez ohledu na atribut **SecurityPolicy** v souboru `qm.ini` . Takže nastavení oprávnění pro jednotlivého uživatele ovlivní pouze tohoto uživatele a ne nikoho jiného, kdo patří do některé ze skupin tohoto uživatele.

Stejně jako u modelu OS má uživatel stále kombinované oprávnění, které bylo přiřazeno jak jednotlivci, tak všem skupinám (pokud existují), do kterých uživatel patří.

Předpokládejme například, že následující záznamy byly definovány v úložišti LDAP.

- Ve třídě **inetOrgPerson** :

```
dn="cn=JohnDoe, ou=users, o=yourcompany, c=yourcountry"
        email=JohnDoe1@yourcompany.com [longer than 12 characters]
        shortu=jodoe
        Phone=1234567
```

- Ve třídě **groupOfNames** :

```
dn="cn=Application Group A, ou=groups, o=yourcompany, c=yourcountry"
        longname=ApplicationGroupA [longer than 12 characters]
```

```
        members="cn=JaneDoe, ou=users, o=yourcompany, c=yourcountry",
                "cn=JohnDoe, ou=users, o=yourcompany, c=yourcountry"
```

Pro účely ověření musí být správce front používající tento server LDAP definován tak, aby jeho hodnota **CONNAUTH** ukazovala na objekt **AUTHINFO** typu IDPWLDAPa jehož příslušné atributy rozlišování názvů jsou pravděpodobně nastaveny takto:

```
USRFIELD(email) SHORTUSR(shortu)
BASEDNU(ou=users,o=yourcompany,c=yourcountry) CLASSUSR(inetOrgPerson)
```

Vzhledem k této konfiguraci pro ověření může aplikace vyplnit pole CSPUserID použité ve volání MQCNO s jednou z následujících sad hodnot:

```
" cn=JohnDoe ", " JohnDoe1@yourcompany.com ", " email=JohnDoe1@yourcompany.com "
```

, nebo

```
" cn=JohnDoe, ou=users, o=ibm, c=uk ", " shortu=jodoe "
```

V obou případech může systém použít dodané hodnoty k ověření kontextu operačního systému " jodoe".

Multi Nastavení autorizací

Jak použijete krátký název nebo **USRFIELD** k nastavení autorizací.

Přístup k práci s více formáty, popsaný v tématu “Autorizace LDAP” na stránce 431, pokračuje v příkazech autorizace, s dalším rozšířením, které může být buď shortname , nebo USRFIELD použito nezdobeným způsobem.

Znakový řetězec určuje konkrétní atribut v záznamu LDAP při pojmenování uživatelů (činitelů) pro autorizaci.

Důležité: Znakový řetězec nesmí obsahovat znak = , protože tento znak nelze použít v ID uživatele operačního systému.

Pokud předáte název činitele do OAM pro autorizaci, která je potenciálně shortname, znakový řetězec se musí vejít do 12 znaků. Algoritmus mapování se nejprve pokusí jej vyřešit na DN pomocí atributu SHORTUSR v dotazu LDAP.

Pokud se to nezdaří s chybou UNKNOWN_ENTITY nebo pokud daný řetězec nemůže být shortname, provede se další pokus o vytvoření dotazu LDAP pomocí atributu USRFIELD.

Upozornění: Pokud jste spustili příkaz DEFINE AUTHINFO, musíte restartovat správce front. Pokud nerestartujete správce front, příkaz setmqaut nevrátí správný výsledek.

Pro zpracování uživatelských autorizací jsou všechna následující nastavení příkazu setmqaut ekvivalentní.

Tabulka 75. Nastavení autorizace uživatele

Příkaz	**Poznámka**
`setmqaut -m QM -t qmgr -p jodoe +connect`	Jedná se o plochý, nekvalifikovaný název, vyřešený pomocí SHORTUSR.
`setmqaut -m QM -t qmgr -pJohnDoe1@yourcompany.com +connect`	Také plochý, nekvalifikovaný název, který se interpretuje přes USRFIELD na stejnou entitu.
`setmqaut -m QM -t qmgr -p email=JohnDoe1@yourcompany.com +connect`	Použití pojmenovaného atributu.

Tabulka 75. Nastavení autorizace uživatele (pokračování)	
Příkaz	**Poznámka**
`setmqaut -m QM -t qmgr -p "phone=1234567" +connect`	Použijte jiný pojmenovaný atribut, který nemusí být žádný z atributů nakonfigurovaných v objektu AUTHINFO.

Jako alternativu k příkazu **setmqaut** můžete použít příkaz SET AUTHREC MQSC:

```
SET AUTHREC OBJTYPE(QMGR) PRINCIPAL('JohnDoe1@yourcompany.com') AUTHADD(connect)
```

nebo příkaz Set Authority Record (MQCMD_SET_AUTH_REC) PCF s prvkem MQCACF_PRINCIPAL_ENTITY_NAMES obsahujícím řetězec:

```
 "cn=JohnDoe,ou=users,o=yourcompany,c=yourcountry"
```

Při zpracování skupin neexistuje žádná nejednoznačnost zpracování `shortname` , protože neexistuje žádný požadavek na přizpůsobení jakékoli formy názvu skupiny do 12 znaků. Proto neexistuje ekvivalent atributu SHORTUSR pro skupiny.

To znamená, že příklady syntaxe popsané v části Tabulka 76 na stránce 433 jsou platné, za předpokladu, že jste nakonfigurovali objekt AUTHINFO s rozšířenými atributy a nastavili jste:

```
GRPFIELD(longname)
BASEDNG(ou=groups,o=yourcompany,c=yourcountry ) CLASSGRP(groupOfNames)
```

Tabulka 76. Nastavení autorizace skupiny	
Příkaz	**Poznámka**
`setmqaut -m QM -t qmgr -g ApplicationGroupA +connect`	Použití GRPFIELD k vyřešení
`setmqaut -m QM -t qmgr -g longname=ApplicationGroupA +connect`	Pojmenování jednoho atributu
`setmqaut -m QM -t qmgr -g "cn=Application Group A,ou=groups,o=yourcompany,c=yourcountry" +connect`	Použití úplného rozlišujícího názvu

Jako alternativu k předcházejícímu příkazu **setmqaut** můžete použít příkaz SET AUTHREC MQSC:

```
SET AUTHREC OBJTYPE(QMGR) GROUP('ApplicationGroupA')
      AUTHADD(connect)
```

nebo příkaz Set Authority Record (MQCMD_SET_AUTH_REC) PCF s prvkem MQCACF_GROUP_ENTITY_NAMES obsahujícím řetězec:

```
 "ApplicationGroupA"
```

Důležité:

Bez ohledu na formát, který používáte k odkazování na název, ať už pro uživatele nebo skupinu, musí být možné odvodit jedinečné DN.

Takže například nesmíte mít dva odlišné záznamy, které mají oba "`shortu=jodoe`".

Pokud nelze určit jediné jedinečné DN, OAM vrátí MQRC_UNKNOWN_ENTITY.

Multi Zobrazení autorizací

Různé metody zobrazení oprávnění uživatelů nebo skupin.

příkaz dspmqaut

Nejjednodušší metodou zobrazení autorizací dostupných pro uživatele nebo skupinu je použití příkazu dspmqaut .

Můžete použít dotaz na libovolnou variantu syntaxe pro identifikaci uživatele nebo skupiny. Všimněte si, že výstup příkazu opakuje identitu ve formátu uvedeném na příkazovém řádku. Výstup neuvádí úplné rozlišené DN.

Příklad:

```
dspmqaut -m QM -t qmgr -p johndoe
Entity johndoe has the following authorizations for object QM:
    connect
```

, nebo

```
dspmqaut -m QM -t qmgr -p email=JohnDoe1@yourcompany.com
Entity email=JohnDoe1@yourcompany.com has the following authorizations for object QM:
    connect
```

příkazy dmpmqaut a dmpmqcfg

Příkaz dmpmqaut a jeho ekvivalenty MQSC nebo PCF mohou určit činitele nebo skupinu v libovolném podporovaném formátu, jako jsou tabulky **setmqaut** popsané v části “Nastavení autorizací” na stránce 432. Avšak na rozdíl od **dspmqaut**příkaz **dmpmqaut** vždy hlásí úplné DN.

```
dmpmqaut -m QM -t qmgr -p jodoe
------------------------------------
profile: self
object type:qmgr
entity:cn=JohnDoe, ou=users, o=yourcompany, c=yourcountry
entity type: principal
authority: connect
```

Podobně příkaz dmpmqcfg , který nemá žádné filtrování vybraných záznamů, vždy zobrazuje úplné DN ve formátu, který lze později přehrát.

```
dmpmqcfg -m QM -x authrec
------------------------------------
SET AUTHREC PROFILE(SELF) +
    PRINCIPAL('cn=JohnDoe, ou=users, o=yourcompany, c=yourcountry') +
    OBJTYPE(QMGR)
    AUTHADD(CONNECT)
```

Multi Další aspekty při použití autorizace LDAP

Stručný popis změn rozhraní MQI (Message Queue Interface) a dalších příkazů MQSC a PCF, které musíte mít na paměti při použití autorizace LDAP z produktu IBM MQ 9.0.0.

ADOPTCTX

Neexistuje žádný požadavek, aby aplikace poskytovaly ověřovací informace, nebo aby byl atribut ADOPTCTX nastaven na hodnotu YES.

Pokud se aplikace explicitně neověřuje nebo pokud je parametr **ADOPTCTX** pro aktivní objekt CONNAUTH nastaven na hodnotu NO , je kontext identity přidružený k aplikaci převzat z ID uživatele operačního systému.

Je-li třeba použít autorizace, je tento kontext mapován na identitu LDAP pomocí stejných pravidel jako pro příkazy setmqaut .

Vstupní parametry pro volání MQI

MQOPEN, MQPUT1a MQSUB mají struktury, které umožňují zadat alternativní ID uživatele.

Pokud jsou tato pole použita, 12znakové ID uživatele je mapováno na DN pomocí stejných pravidel jako v příkazech **setmqaut**, **dmpmqaut**a **dspmqaut** .

Příkazy MQPUT a MQPUT1 také umožňují vhodně autorizovaným programům nastavit pole MQMD UserIdentifier . Hodnota tohoto pole není během procesu PUT policed a lze ji nastavit na libovolnou hodnotu.

Jako obvykle však lze hodnotu **UserIdentifier** použít pro autorizaci v pozdějších fázích zpracování zprávy, například když je v přijímacím kanálu definována hodnota PUTAUT (CTX).

V tomto bodě bude zkontrolována autorizace identifikátoru s použitím konfigurace přijímajícího správce front, který může být založen na protokolu LDAP nebo na operačním systému.

Výstupní parametry pro volání MQI

Kdykoli je programu poskytnuto ID uživatele ve struktuře MQI, jedná se o 12znakovou verzi krátkého názvu přidruženou k připojení.

Například hodnota **MQAXC.UserId** pro uživatelské procedury rozhraní API je krátký název vrácený z mapování LDAP.

Další administrativní příkazy MQSC a PCF

Příkazy, které zobrazují informace o uživateli ve stavu objektu, jako např. DISPLAY CONN USERID , vracejí 12znakový krátký název přidružený ke kontextu. Úplné DN není zobrazeno.

Příkazy, které umožňují deklaraci identit, jako např. pravidla mapování CHLAUTH nebo hodnoty MCAUSER pro kanály, mohou mít hodnoty až do maximální délky definované pro tyto atributy (momentálně 64 znaků).

Syntaxe se nemění. Když je pro tuto identitu vyžadována autorizace, je interně mapována na DN pomocí stejných pravidel jako pro příkazy **setmqaut**, **dmpmqaut**a **dspmqaut** .

To znamená, že hodnota MCAUSER v definici kanálu se nemusí zobrazit jako stejný řetězec jako DISPLAY CHSTATUS , ale odkazují na stejnou identitu.

Příklad:

```
DEFINE CHL(SV1) CHLTYPE(SVRCONN) MCAUSER('cn=JohnDoe')
DEFINE CHL(SV2) CHLTYPE(SVRCONN) MCAUSER('jodoe')
DEFINE CHL(SV3) CHLTYPE(SVRCONN) MCAUSER('JohnDoe1@yourcompany.com')
```

Pak příkaz DISPLAY CHSTATUS (*) ALL zobrazí hodnotu SHORTUSR, *MCAUSER (jodoe)* pro všechna připojení.

Multi Přepínání mezi modely autorizace OS a LDAP

Způsob přepínání mezi různými metodami autorizace na různých platformách.

Atribut CONNAUTH správce front ukazuje na objekt AUTHINFO. Když je objekt typu IDPWLDAP, použije se pro ověření úložiště LDAP.

Nyní můžete použít metodu autorizace na stejný objekt, která vám umožní pokračovat s autorizací založenou na OS, nebo pracovat s autorizací LDAP.

IBM i, AIX and Linux

Linux IBM i AIX

Správce front lze kdykoli přepínat mezi modely OS a LDAP. Konfiguraci můžete změnit a aktivovat ji pomocí příkazu REFRESH SECURITY TYPE (CONNAUTH) .

Například, pokud byl tento objekt již nakonfigurován s informacemi o připojení pro ověření:

```
ALTER AUTHINFO(MYLDAP) AUTHTYPE(IDPWLDAP) +
        AUTHORMD(SEARCHGRP) +
        BASEDNG('ou=groups,o=ibm,c=uk') +
        <other attributes>
ALTER QMGR CONNAUTH(MYLDAP)
REFRESH SECURITY
```

Windows

Windows

Pokud změna konfigurace oprávnění zahrnuje přepínání mezi modely OS a LDAP, musí být restartován správce front, aby se změna projevila. Jinak můžete změnu aktivovat pomocí příkazu REFRESH SECURITY TYPE (CONNAUTH) .

Pravidla zpracování

Při přepínání z OS na autorizaci LDAP se všechna existující pravidla oprávnění operačního systému, která byla nastavena, stanou neaktivními a neviditelnými.

Příkazy, jako např. **dmpmqaut** , tato pravidla OS nezobrazují. Podobně při zpětném přepnutí z LDAP na OS se jakákoli definovaná oprávnění LDAP stanou neaktivní a neviditelná, čímž se obnoví původní pravidla OS.

Chcete-li z jakéhokoli důvodu zálohovat definice správce front pomocí příkazu **dmpmqcfg** , bude tato záloha obsahovat pouze ta pravidla, která jsou definována pro metodu autorizace, která byla v době zálohování platná.

Multi Administrace LDAP

Přehled toho, jak každá platforma spravuje LDAP.

Při použití autorizace LDAP není členství ve skupině `mqm` (nebo ekvivalentní skupině) v operačním systému tak důležité. Je-li členem této skupiny, řídí pouze to, zda mohou být zpracovány určité příkazy příkazového řádku.

Konkrétně musíte být v této skupině, abyste mohli zadat příkazy strmqm a endmqm .

Jakmile je správce front spuštěn, existují nyní limity pro plně privilegovaný účet. Kromě ID uživatele osoby, která zadala příkaz **strmqm** , nezískají další uživatelé patřící do skupiny OS `mqm` (nebo ekvivalentní skupiny) speciální oprávnění.

Autorizace ostatních uživatelů jsou založeny na tom, ke kterým skupinám LDAP patří. Nekvalifikované použití názvu skupiny `mqm` v příkazech, jako je **setmqaut** , není povoleno mapovat na žádnou skupinu LDAP.

AIX and Linux

Linux AIX

Po spuštění správce front je jediným automaticky plně privilegovaným účtem skutečný uživatel, který spustil správce front.

ID mqm stále existuje a používá se jako vlastník prostředků operačního systému, například souborů, protože mqm je efektivní ID, pod kterým je spuštěn správce front. Uživatel mqm však nebude moci automaticky provádět administrativní úlohy řízené modulem OAM.

Windows

Windows

V systému Windowsjsou automaticky plně oprávněnými účty uživatel operačního systému, který spustil správce front, a také uživatel, který spustil procesy jádra správce front, například MUSR_MQADMIN, pokud byl správce front spuštěn jako služba systému Windows .

Při spuštění v režimu autorizace LDAP se produkt Windows chová velmi podobně jako platformy AIX and Linux . Zabývá se krátkými jmény 12 znaků a plnými DN.

IBM i

IBM i

V systému IBM ijsou automaticky privilegované účty ty, které spouští správce front a ID QMQM.

Potřebujete obě ID, protože ID uživatele, který spouští správce front, je vyžadováno pouze ke spuštění systému. Po spuštění mají procesy správce front pouze oprávnění QMQM.

Ukázkový skript pro poskytnutí oprávnění MQADMIN

Linux AIX

Vzhledem k tomu, že je užitečné mít skupinu schopnou provádět úplnou administraci ve správci front, je ukázkový skript na platformách AIX and Linux dodáván jako:

```
MQ_INSTALLATION_PATH/samp/bin/amqauthg.sh
```

Tato ukázka má dva parametry:

- Název správce front
- Název skupiny LDAP

Ukázkové procesy zpracují příkazy setmqaut a udělí úplné oprávnění pro všechny objekty. Jedná se o stejný skript, který je vygenerován průvodcem OAM IBM MQ Explorer pro administrativní role. Kód například začíná:

```
setmqaut -t q -m qmgr -n "**" +alladm -g
      groupname
```

Důvěrnost zpráv

Šifrování zpráv zajišťuje, že obsah zpráv zůstane důvěrný. Existují různé metody šifrování zpráv v produktu IBM MQ v závislosti na vašich potřebách.

Potřebujete-li komplexní ochranu dat na úrovni aplikace pro infrastrukturu systému zpráv typu point-to-point, můžete použít Advanced Message Security k šifrování zpráv nebo napsat vlastní uživatelskou proceduru rozhraní API nebo uživatelskou proceduru přechodu rozhraní API.

Nejbezpečnějším řešením je poskytnout komplexní šifrování zašifrováním zprávy od bodu, kdy je vložena aplikací, do bodu, kde je získána přijímající aplikací. To lze provést pomocí produktu “Plánování pro Advanced Message Security” na stránce 108 (AMS) nebo napsáním vlastní uživatelské procedury rozhraní API nebo křížové uživatelské procedury rozhraní API; další informace viz “Implementace důvěrnosti v uživatelských programech” na stránce 485 .

Potřebujete-li šifrovat zprávy pouze v době, kdy jsou přenášeny přes síť, můžete použít protokol TLS; další informace naleznete v části “Protokoly zabezpečení TLS v adresáři IBM MQ” na stránce 24 nebo můžete

napsat vlastní uživatelskou proceduru pro zabezpečení zprávy, uživatelskou proceduru pro zprávy nebo uživatelské programy pro odeslání a příjem k provedení šifrování.

z/OS Potřebujete-li šifrovat zprávy v klidu ve správci front, můžete použít šifrování datové sady z/OS pro tohoto správce front; další informace naleznete v části “Důvěrnost pro data v klidu na serveru IBM MQ for z/OS se šifrováním datové sady” na stránce 486 .

Související úlohy

Připojení dvou správců front pomocí protokolu TLS

Bezpečné připojení klienta ke správci front

Povolení CipherSpecs

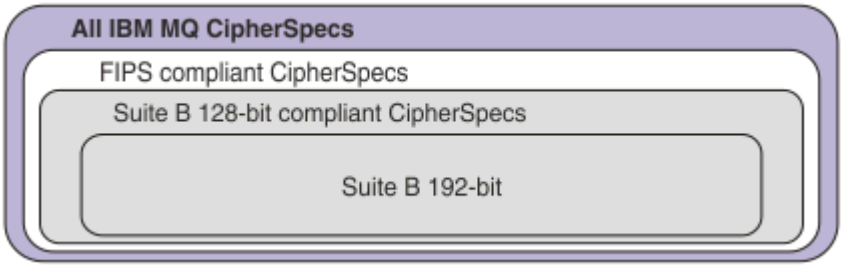
Povolte CipherSpec pomocí parametru **SSLCIPH** v příkazu **DEFINE CHANNEL** nebo **ALTER CHANNEL** MQSC.

Poznámka: V systému AIX, Linux, and Windowsposkytuje produkt IBM MQ kompatibilitu se standardem FIPS 140-2 prostřednictvím šifrovacího modulu IBM Crypto for C (ICC) . Certifikát pro tento modul byl přesunut do historického stavu. Zákazníci by si měli prohlédnout IBM Crypto for C (ICC) certifikát a měli by si být vědomi všech doporučení poskytnutých NIST. Náhradní modul FIPS 140-3 momentálně probíhá a jeho stav lze zobrazit jeho vyhledáním v modulech NIST CMVP v seznamu procesů.

Některé ze specifikací CipherSpecs , které můžete použít s produktem IBM MQ , vyhovují standardu FIPS. Některé CipherSpecs vyhovující standardu FIPS jsou také kompatibilní se standardem Suite B, i když jiné, jako například TLS_RSA_WITH_AES_256_CBC_SHA, nejsou.

Všechny CipherSpecs vyhovující standardu Suite B jsou také kompatibilní se standardem FIPS. Všechny specifikace CipherSpecs vyhovující standardu Suite B spadají do dvou skupin: 128 bitů (například ECDHE_ECDSA_AES_128_GCM_SHA256) a 192 bitů (například ECDHE_ECDSA_AES_256_GCM_SHA384),

Následující diagram ilustruje vztah mezi těmito dílčími sadami:



V produktu IBM MQ 9.2.0produkt podporuje protokol zabezpečení TLS 1.3 na všech platformách.

CipherSpecs , které můžete použít pro každou z těchto platforem, jsou uvedeny v části Tabulka 77 na stránce 439. Informace o použití těchto specifikací CipherSpecsnaleznete v části “Použití TLS 1.3 v IBM MQ” na stránce 441 a “IBM MQ MQI client a TLS 1.3” na stránce 442.

Pro usnadnění konfigurace a budoucí migrace poskytuje produkt IBM MQ také sadu aliasů CipherSpecs. Migrace existujících konfigurací zabezpečení pro použití aliasu CipherSpec znamená, že se můžete přizpůsobit dodatkům šifer a zamítnutí, aniž byste v budoucnu museli provádět další invazivní změny konfigurace. Tyto alias CipherSpecs jsou uvedeny v části Alias CipherSpecs v souboru Tabulka 77 na stránce 439. Další informace o migraci pro použití aliasu CipherSpecnaleznete v tématu Migrace existujících konfigurací zabezpečení pro použití aliasu CipherSpec.

Můžete nakonfigurovat výchozí CipherSpecs , jak je popsáno v tématu “Výchozí hodnoty CipherSpec jsou povoleny v produktu IBM MQ” na stránce 442. Můžete také poskytnout alternativní sadu CipherSpecs , které jsou povoleny pro použití s kanály na:

- Multi IBM MQ for Multiplatforms, jak je popsáno v tématu “Poskytnutí vlastního seznamu seřazených a povolených CipherSpecs na systému IBM MQ for Multiplatforms” na stránce 451.

- z/OS IBM MQ for z/OS, jak je popsáno v tématu “Poskytnutí vlastního seznamu seřazených a povolených CipherSpecs na systému IBM MQ for z/OS” na stránce 452.

Zamítnuté specifikace CipherSpecs , které můžete v případě potřeby znovu povolit pro použití s produktem IBM MQ , jsou uvedeny v části “Zamítnuté specifikace CipherSpecs” na stránce 453. Informace o povolení zamítnutých specifikací CipherSpecsviz “Povolení zamítnutých specifikací CipherSpecs na systému IBM MQ for Multiplatforms” na stránce 456 nebo “Povolení zamítnutých specifikací CipherSpecs na systému z/OS” na stránce 457.

CipherSpecs , které můžete použít s podporou protokolu IBM MQ TLS.

V následující tabulce jsou uvedeny specifikace CipherSpecs , které můžete automaticky používat se správcem front IBM MQ . Požadujete-li osobní certifikát, určíte velikost klíče pro dvojici veřejný a soukromý klíč. Velikost klíče, která se používá během navázání komunikace TLS, je velikost uložená v certifikátu, pokud není určena CipherSpec, jak je uvedeno v tabulce.

Tabulka 77. Specifikace šifrování, které lze použít s podporou TLS produktu IBM MQ

Podpora platformy “1” na stránce 441	**Název specifikace šifrování**	**Hexadecimální kód**	**Použitý protokol**	**Algoritmus MAC**	**Šifrovací algoritmus (šifrovací bity)**	**FIPS** “2” na stránce 441	**Suite B**
Specifikace CipherSpecs aliasu							
Vše	ANY_TLS13_OR_HIGHER “3” na stránce 441 “4” na stránce 441	Není k dispozici	Dohodnuto	Dohodnuto	Dohodnuto	Dohodnuto	Dohodnuto
Vše	ANY_TLS13 “4” na stránce 441 “5” na stránce 441	Není k dispozici	TLS 1.3	Dohodnuto	Dohodnuto	Dohodnuto	Dohodnuto
Vše	ANY_TLS12_OR_HIGHER “4” na stránce 441 “6” na stránce 441	Není k dispozici	Dohodnuto	Dohodnuto	Dohodnuto	Dohodnuto	Dohodnuto
Vše	ANY_TLS12 “7” na stránce 441	Není k dispozici	TLS 1.2	Dohodnuto	Dohodnuto	Dohodnuto	Dohodnuto
Vše	ANY “8” na stránce 441	Není k dispozici	Dohodnuto	Dohodnuto	Dohodnuto	Dohodnuto	Dohodnuto
CipherSpecs pro TLS 1.3							
Vše	TLS_AES_128_GCM_SHA256	1301	TLS 1.3	GCM	AES-128 s volbou GCM (128)	Ano	Ne
Vše	TLS_AES_256_GCM_SHA384	1302	TLS 1.3	GCM	AES-256 s GCM (256)	Ano	Ne
Vše	TLS_CHACHA20_POLY1305_SHA256	1303	TLS 1.3	POLY1305	CHACHA20 (256)	Ne	Ne
ALW	TLS_AES_128_CCM_SHA256	1304	TLS 1.3	CBC-MAC	AES-128 s CTR (128)	Ano	Ne

Tabulka 77. Specifikace šifrování, které lze použít s podporou TLS produktu IBM MQ (pokračování)

Podpora platformy "1" na stránce 441	Název specifikace šifrování	Hexadecimální kód	Použitý protokol	Algoritmus MAC	Šifrovací algoritmus (šifrovací bity)	FIPS "2" na stránce 441	Suite B
ALW	TLS_AES_128_CCM_8_SHA256 "10" na stránce 441	1305	TLS 1.3	CBC-MAC	AES-128 s CTR (128)	Ano	Ne
CipherSpecs pro TLS 1.2							
Vše	TLS_RSA_WITH_AES_128_CBC_SHA256 "9" na stránce 441	003C	TLS 1.2	SHA-256	AES (128)	Ano	Ne
Vše	TLS_RSA_WITH_AES_256_CBC_SHA256 "9" na stránce 441 "11" na stránce 441	003D	TLS 1.2	SHA-256	AES (256)	Ano	Ne
Vše	TLS_RSA_WITH_AES_128_GCM_SHA256 "9" na stránce 441 "12" na stránce 441	009C	TLS 1.2	SHA-256 a AEAD GCM	AES (128)	Ano	Ne
Vše	TLS_RSA_WITH_AES_256_GCM_SHA384 "9" na stránce 441 "11" na stránce 441 "12" na stránce 441	009D	TLS 1.2	SHA-384 a AEAD GCM	AES (256)	Ano	Ne
Vše	ECDHE_ECDSA_AES_128_CBC_SHA256 "9" na stránce 441	C023	TLS 1.2	SHA-256	AES (128)	Ano	Ne
Vše	ECDHE_ECDSA_AES_256_CBC_SHA384 "9" na stránce 441 "11" na stránce 441	C024	TLS 1.2	SHA-384	AES (256)	Ano	Ne
Vše	ECDHE_RSA_AES_128_CBC_SHA256 "9" na stránce 441	C027	TLS 1.2	SHA-256	AES (128)	Ano	Ne
Vše	ECDHE_RSA_AES_256_CBC_SHA384 "9" na stránce 441 "11" na stránce 441	C028	TLS 1.2	SHA-384	AES (256)	Ano	Ne
Multi	ECDHE_ECDSA_AES_128_GCM_SHA256 "11" na stránce 441 "12" na stránce 441	C02B	TLS 1.2	SHA-256 a AEAD GCM	AES (SHA384)	Ano	128bitové
Multi	ECDHE_ECDSA_AES_256_GCM_SHA384 "11" na stránce 441 "12" na stránce 441	C02C	TLS 1.2	SHA-384 a AEAD GCM	AES (SHA384)	Ano	192bitové
Vše	ECDHE_RSA_AES_128_GCM_SHA256 "12" na stránce 441	C02F	TLS 1.2	SHA-256 a AEAD GCM	AES (128)	Ano	Ne
Vše	ECDHE_RSA_AES_256_GCM_SHA384 "11" na stránce 441 "12" na stránce 441	C030	TLS 1.2	AEAD AES-128 GCM	AES (SHA384)	Ano	Ne

Tabulka 77. Specifikace šifrování, které lze použít s podporou TLS produktu IBM MQ (pokračování)

Podpora platformy "1" na stránce 441	Název specifikace šifrování	Hexadecimální kód	Použitý protokol	Algoritmus MAC	Šifrovací algoritmus (šifrovací bity)	FIPS "2" na stránce 441	Suite B

Notes:

1. Seznam platforem pokrytých každou ikonou platformy naleznete v tématu Ikony použité v dokumentaci k produktu.
2. Uvádí, zda má specifikace šifrování certifikaci FIPS na platformě s certifikací FIPS. Vysvětlení FIPS viz Federal Information Processing Standards (FIPS).
3. ALW Alias ANY_TLS13_OR_HIGHER šifrování CipherSpec vyjedná nejvyšší úroveň zabezpečení, kterou vzdálený konec umožní, ale připojí se pouze protokolem TLS 1.3 nebo vyšším.
4. IBM i Chcete-li použít protokol TLS 1.3 nebo ANY CipherSpec v IBM i, musí základní verze operačního systému podporovat TLS 1.3. Další informace viz Podpora TLS systému pro TLSv1.3.
5. ALW Specifikace ANY_TLS13 CipherSpec představuje podmnožinu přijatelných specifikací CipherSpecs, které používají protokol TLS 1.3, jak je uvedeno v této tabulce pro jednotlivé platformy.
6. ALW Alias ANY_TLS12_OR_HIGHER šifrování CipherSpec vyjedná nejvyšší úroveň zabezpečení, kterou vzdálený konec umožní, ale připojí se pouze protokolem TLS 1.2 nebo vyšším.
7. Specifikace ANY_TLS12 CipherSpec představuje podmnožinu přijatelných specifikací CipherSpecs, které používají protokol TLS 1.2, jak je uvedeno v této tabulce pro jednotlivé platformy.
8. ALW Alias ANY šifrování CipherSpec vyjedná nejvyšší úroveň zabezpečení, kterou vzdálený konec umožní.
9. IBM i Tyto specifikace CipherSpecs nejsou povoleny v systémech IBM i 7.4, které mají hodnotu systému QSSLCSLCTL nastavenou na *OPSSYS.
10. ALW Tato šifrování CipherSpecs používají 8oktetovou hodnotu ICV (8-octet Integrity Check Value) namísto 16oktetové hodnoty ICV.
11. Tuto specifikaci šifrování nelze použít k zabezpečení připojení z produktu IBM MQ Explorer na správce front, pokud nebudou v prostředí JRE průzkumníkem Explorer použity příslušné soubory neomezených zásad.
12. ALW Podle doporučení GSKit, TLS 1.2 GCM CipherSpecs mají omezení, což znamená, že po odeslání záznamů TLS24.5 s použitím stejného klíče relace je připojení ukončeno zprávou AMQ9288E. Toto omezení GCM je aktivní, bez ohledu na použitý režim FIPS.

    Chcete-li zabránit výskytu této chyby, vyhněte se použití šifer TLS 1.2 GCM , povolte reset tajného klíče nebo spusťte správce front nebo klienta IBM MQ s nastavenou proměnnou prostředí `GSK_ENFORCE_GCM_RESTRICTION=GSK_FALSE` . V případě knihoven GSKit musíte tuto proměnnou prostředí nastavit na obou stranách připojení a použít ji na připojení klienta ke správci front i na připojení správce front. Všimněte si, že toto nastavení ovlivňuje nespravované klienty .NET , ale ne Java nebo spravované .NET klienty. Další informace viz AES-GCM omezení šifrování.

    Toto omezení se nevztahuje na IBM MQ for z/OS.

Použití TLS 1.3 v IBM MQ

V systému IBM MQ 9.2.0produkt podporuje protokol TLS 1.3 na všech platformách. Před IBM MQ 9.2.0, byla podpora TLS 1.3 k dispozici na AIX, Linux, and Windows pro Continuous Delivery z IBM MQ 9.1.4.

Správci front, kteří jsou vytvořeni v produktu IBM MQ 9.2.0 nebo novější, standardně podporují protokol TLS 1.3 . Správci front migrovaní ze starších verzí produktu IBM MQ musí mít povoleno zabezpečení TLS 1.3 . Protokol TLS 1.3 můžete u migrovaných správců front povolit nastavením vlastnosti **AllowTLSV13**=TRUE :

- Multi Pro správce front IBM MQ for Multiplatforms upravte soubor `qm.ini` a přidejte vlastnost **AllowTLSV13**=TRUE pod sekci SSL (odkaz na

```
SSL:
  AllowTLSV13=TRUE
```

- z/OS Pro správce front IBM MQ for z/OS upravte datovou sadu QMINI určenou v JCL spuštění správce front a přidejte vlastnost **AllowTLSV13**=TRUE pod sekci TransportSecurity .

```
TransportSecurity:
    AllowTLSV13=TRUE
```

Když je povolen protokol TLS 1.3 a v souladu se specifikací TLS 1.3, jakýkoli pokus o komunikaci se slabou specifikací CipherSpec, bez ohledu na to, zda jsou povoleny v produktu IBM MQ či nikoli, je odmítnut. CipherSpecs , které TLS 1.3 považuje za slabé, jsou CipherSpecs , které splňují jedno nebo více z následujících kritérií:

- Používá protokol SSL 3.0 .
- Jako šifrovací algoritmus používá RC4 nebo RC2 .
- Má velikost šifrovacího klíče (bit) rovnou nebo menší než 112.

Tato omezení jsou označena poznámkou [3] v tabulce 1 zamítnutých CipherSpecs.

Potřebujete-li pokračovat v používání takových CipherSpecs, musíte zakázat režim TLS 1.3 :

- ALW Upravte soubor `qm.ini` správce front a změňte nastavení vlastnosti **AllowTLSV13** na:

```
SSL:
  AllowTLSV13=FALSE
```

- z/OS Upravte datovou sadu QMINI správce front a změňte nastavení vlastnosti **AllowTLSV13** na:

```
TransportSecurity:
    AllowTLSV13=FALSE
```

IBM MQ MQI client a TLS 1.3

ALW

Při použití IBM MQ MQI clientje hodnota **AllowTLSV13** odvozena, pokud není výslovně uvedena v sekci SSL souboru `mqclient.ini` , který je používán aplikací.

- Pokud jsou povoleny slabé CipherSpecs , je parametr **AllowTLSV13** nastaven na hodnotu FALSE a nelze použít žádný protokol TLS 1.3 CipherSpecs .
- Jinak je parametr **AllowTLSV13** nastaven na hodnotu TRUE a lze použít nové specifikace TLS 1.3 CipherSpecs a alias CipherSpecs .

Výchozí hodnoty CipherSpec jsou povoleny v produktu IBM MQ

Ve výchozí konfiguraci nového správce front IBM MQ poskytuje produkt IBM MQ podporu protokolů TLS 1.2 a TLS 1.3 a různých šifrovacích algoritmů pomocí CipherSpecs. Pro účely kompatibility lze produkt IBM MQ také nakonfigurovat tak, aby používal protokoly SSL 3.0 a TLS 1.0 a řadu šifrovacích algoritmů, o nichž je známo, že jsou slabé nebo náchylné k ohrožení zabezpečení. Seznam CipherSpecs , které jsou povoleny ve výchozí konfiguraci, se může změnit použitím údržby.

Produkt IBM MQ je možné nakonfigurovat tak, aby omezoval nebo povoloval použití CipherSpecs pomocí následujících ovládacích prvků:

- Povolte pouze specifikace CipherSpecs vyhovující standardu FIPS 140-2 pomocí SSLFIPS.
- ALW Povolte pouze CipherSpecs kompatibilní s NSA Suite B pomocí SUITEB.
- Multi Povolte vlastní seznam specifikací CipherSpecs pomocí **AllowedCipherSpecs**.
- ALW Povolte vlastní seznam specifikací CipherSpecs pomocí proměnné prostředí **AMQ_ALLOWED_CIPHERS** .
- ALW Povolte použití zamítnutých specifikací CipherSpecs pomocí **AllowWeakCipher** nebo proměnné prostředí **AMQ_SSL_WEAK_CIPHER_ENABLE** .
- z/OS Povolte použití zamítnutých specifikací CipherSpecs pomocí příkazů DD v JCL CHINIT.

Poznámka: Určíte-li vlastní seznam specifikací CipherSpecs pomocí **AllowedCipherSpecs** nebo **AMQ_ALLOWED_CIPHERS** , potlačí povolení všech zamítnutých specifikací CipherSpecs. Všimněte si, že při použití omezení NSA Suite B nebo FIPS 140-2 v kombinaci s vlastním seznamem CipherSpec se musíte ujistit, že vlastní seznam obsahuje pouze CipherSpecs povolené nastavením sady B nebo FIPS 140-2.

Související pojmy

“Digitální certifikáty a kompatibilita CipherSpec v produktu IBM MQ” na stránce 46
Toto téma poskytuje informace o tom, jak zvolit příslušné specifikace CipherSpecs a digitální certifikáty pro vaši zásadu zabezpečení, a to nastíněním vztahu mezi specifikacemi CipherSpecs a digitálními certifikáty v produktu IBM MQ.

“CipherSpecs a CipherSuites” na stránce 21
Šifrovací bezpečnostní protokoly se musí dohodnout na algoritmech používaných zabezpečeným připojením. CipherSpecs a CipherSuites definují specifické kombinace algoritmů.

“Konfigurace produktu IBM MQ pro sadu B” na stránce 43
Produkt IBM MQ lze nakonfigurovat tak, aby fungoval v souladu se standardem NSA Suite B na platformách AIX, Linux, and Windows .

“Federální standardy zpracování informací (FIPS)” na stránce 33
Toto téma představuje program FIPS (Federal Information Processing Standards) Cryptomodule Validation Program Národního institutu pro standardy a technologie USA a šifrovací funkce, které lze použít na kanálech TLS.

Související úlohy

Migrace existujících konfigurací zabezpečení pro použití aliasu CipherSpe

Související odkazy

Definovat kanál

POZMĚNIT KANÁL

Změnit, kopírovat a vytvořit kanál

ALW AES-omezení šifrováníGCM

Průvodce omezeními, která jsou uložena pro šifry AES-GCM , když jsou použity pro šifrování TLS. Tato omezení jsou zavedena organizacemi IETF a NIST a vyžadují, aby stejný klíč relace nebyl použit k bezpečnému přenosu více než $2^{24.5}$ záznamů TLS při použití šifer AES-GCM .

Další informace o těchto omezeních viz Sekce RFC 9325 4.4 Omezení použití klíče a Sekce RFC 8446 5.5.

Produkt IBM MQ přímo neimplementuje šifrovací funkčnost. Místo toho se k zajištění funkcí TLS a Advanced Message Security používá několik různých šifrovacích knihoven. V operačních systémech Windows, Linuxa AIX je šifrovací knihovna, kterou IBM MQ používá, IBM Global Security Kit (GSKit). V případě aplikací knihovny C a nespravované knihovny .NET používají GSKit pro šifrovací funkčnost. Implementace šifrovacích algoritmů AES-GCM podle produktu GSKit zahrnuje omezení uvedená skupinou standardů. Tato omezení jsou také standardně povolena. Jako taková je komunikace IBM MQ TLS, když

používáte šifry AES-GCM , ukončena, pokud jsou více než $2^{24.5}$ záznamy TLS přeneseny pomocí stejného klíče relace.

Poznámka: Toto omezení není přítomno na platformách IBM i, IBM Z nebo IBM MQ for HPE NonStop nebo Java/JMS, spravovaných .NET aplikacích, protože se používají různé šifrovací knihovny a tyto knihovny neimplementovaly stejné omezení.

Pokud kanál IBM MQ zůstane spuštěn dostatečně dlouho, aby byly pomocí stejného klíče relace přeneseny více než 2 záznamy TLS$^{24.5}$, základní šifrovací knihovna ukončí připojení. To způsobí ukončení kanálu a vygeneruje se chybová zpráva AMQ9288E . Aplikace, jejichž komunikace byla tímto způsobem ukončena, obdrží návratový kód `MQRC_CONNECTION_BROKEN` z operace IBM MQ , která byla provedena.

Ukončení připojení lze provést na obou koncích komunikace, ale pouze na koncích, které používají produkt GSKit pro šifrovací funkčnost.

Doporučení pro zmírnění omezení

Některé volby, jak zabránit nebo zacházet s komunikacemi, které jsou ukončeny kvůli tomuto omezení, jsou následující:

Použít znovu připojitelné klienty
Aplikace lze konfigurovat tak, aby se v případě selhání připojení automaticky pokusily o opětovné připojení. To zahrnuje připojení ukončená kvůli omezení GCM . Při konfiguraci pro opětovné připojení je klientská aplikace automaticky obnovena v libovolném bodě selhání a všechny popisovače pro otevření objektů jsou obnoveny. To se provádí bez návratu do kódu aplikace.

Další informace naleznete v tématu Automatické opětovné připojení klienta.

Nastavit hodnotu resetování tajného klíče
Produkt IBM MQ lze nakonfigurovat tak, aby požadoval reset klíče relace po přenesení konfigurovatelného počtu bajtů přes kanál. Po dosažení tohoto limitu produkt IBM MQ požaduje, aby šifrovací vrstva provedla reset klíče relace, což povede k novému klíči relace.

Je důležité si uvědomit, že uvedená hodnota je počet přenesených bajtů, který souvisí s velikostí zpráv odesílaných produktem IBM MQ. Omezení je na počtu záznamů TLS, které se odešlou. Neexistuje přímé mapování mezi bajty zpráv a záznamy TLS, protože záznam TLS může odeslat maximální počet bajtů závislých na MTU (Maximum Transmission Unit) sítě. Všechny odeslané zprávy, které jsou větší než tato hodnota, jsou přenášeny jako více záznamů TLS. Hodnota MTU se mezi sítěmi liší. Existují také další důvody, proč může být nutné odeslat záznam TLS mimo přenos dat zprávy IBM MQ , například IBM MQ Kontroly prezenčního signálu, výstrahy TLS, další zprávy protokolu IBM MQ . Tyto další záznamy TLS se počítají k maximálnímu počtu záznamů TLS, ale nejsou započítány v hodnotě resetu tajného klíče IBM MQ .

Pravidelné resetování klíče relace pomocí resetu tajného klíče může zabránit ukončení kanálu kvůli omezení AES-GCM .

Další informace viz Resetování tajných klíčů SSL a TLS.

Použít specifikace šifrování TLS 1.3
Zatímco omezení AES-GCM je stále přítomno při použití protokolu TLS 1.3 , protokol TLS 1.3 podporuje automatické provedení resetování klíče relace bez nutnosti přerušit komunikaci TLS. To umožňuje produktu GSKit spravovat resetování klíče relace, když je to nezbytné, aniž by produkt IBM MQ musel požadovat reset tajného klíče.

Další informace viz Použití TLS 1.3 v IBM MQ v “Povolení CipherSpecs” na stránce 438.

Zakázat omezení AES-GCM
V případě potřeby lze omezení zakázat nastavením proměnné prostředí **`GSK_ENFORCE_GCM_RESTRICTION=GSK_FALSE`** tak, aby zakázala omezení AES-GCM . Tímto způsobem lze pomocí stejného klíče relace odeslat libovolný počet záznamů TLS. Zvolíte-li toto zmírnění, proměnná prostředí musí být nastavena na každém konci komunikace, která používá GSKit pro zabezpečené komunikace.

Upozornění: Tato volba se nedoporučuje, protože po odeslání více než 2 záznamů TLS[24.5] je možné, aby útočníci provedli analýzu odeslaných záznamů a určili používaný klíč relace. Jakmile je klíč relace určen, je ohrožena veškerá existující a budoucí komunikace pomocí tohoto klíče relace.

Pořadí CipherSpec v navázání komunikace TLS

Pořadí CipherSpecs se používá při výběru mezi více možnými specifikacemi CipherSpecs, například při použití jedné ze specifikací ANY* CipherSpecs.

Během navázání komunikace TLS si klient a server vyměňují specifikace CipherSpecs a protokoly, které podporují, v pořadí podle svých preferencí. Pro komunikaci TLS je vybrána a použita společná CipherSpec , které obě strany určují prioritu. Při výběru protokolu CipherSpec se bere v úvahu i verze, například pokud server vypisuje protokol TLS 1.2 CipherSpecs před protokolem TLS 1.3 CipherSpecs , bude i nadále určovat prioritu protokolu TLS 1.3 , pokud jej klient podporuje a má k dispozici běžný protokol TLS 1.3 CipherSpec , který lze použít.

V produktu IBM MQ 9.2.0, když je produkt IBM MQ nakonfigurován pro TLS, nastaví CipherSpecs v pořadí uvedeném v následující tabulce, od nejpreferovanějšího po nejméně preferovaný.

Poznámka: Pokud není volba CipherSpec povolena prostřednictvím atributu **AllowedCipherSpecs** , nebude konfigurována pro použití během navázání komunikace TLS.

V případě, že atribut **AllowedCipherSpecs** není uveden, použije se výchozí seznam povolených šifer označených následující tabulkou.

Tabulka 78. Pořadí CipherSpecs od IBM MQ 9.2.0

Platforma	CipherSpec	Protokol	Hexadecimální kód	Standardně povoleno
Vše	TLS_CHACHA20_POLY1305_SHA256	TLS 1.3	1303	Ano
Vše	TLS_AES_256_GCM_SHA384	TLS 1.3	1302	Ano
Vše	TLS_AES_128_GCM_SHA256	TLS 1.3	1301	Ano
ALW	TLS_AES_128_CCM_SHA256	TLS 1.3	1304	Ano
ALW	TLS_AES_128_CCM_8_SHA256	TLS 1.3	1305	Ano
Vše	TLS_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2	009D	Ano
Multi	ECDHE_ECDSA_AES_256_GCM_SHA384	TLS 1.2	C02C	Ano
Vše	ECDHE_RSA_AES_256_GCM_SHA384	TLS 1.2	C030	Ano
Vše	TLS_RSA_WITH_AES_256_CBC_SHA256	TLS 1.2	003D	Ano
Vše	ECDHE_ECDSA_AES_256_CBC_SHA384	TLS 1.2	C024	Ano

Tabulka 78. Pořadí CipherSpecs od IBM MQ 9.2.0 (pokračování)				
Platforma	**CipherSpec**	**Protokol**	**Hexadecimální kód**	**Standardně povoleno**
Vše	ECDHE_RSA_AES_256_CBC_SHA384	TLS 1.2	C028	Ano
Vše	TLS_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2	009C	Ano
Multi	ECDHE_ECDSA_AES_128_GCM_SHA256	TLS 1.2	C02B	Ano
Vše	ECDHE_RSA_AES_128_GCM_SHA256	TLS 1.2	C02F	Ano
Vše	TLS_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2	003C	Ano
Vše	ECDHE_ECDSA_AES_128_CBC_SHA256	TLS 1.2	C023	Ano
Vše	ECDHE_RSA_AES_128_CBC_SHA256	TLS 1.2	C027	Ano
ALW	ECDHE_ECDSA_3DES_EDE_CBC_SHA256	TLS 1.2	C008	Ne
Multi	ECDHE_RSA_3DES_EDE_CBC_SHA256	TLS 1.2	C012	Ne
ALW	TLS_RSA_WITH_RC4_128_SHA256	TLS 1.2	0005	Ne
ALW	ECDHE_ECDSA_RC4_128_SHA256	TLS 1.2	C007	Ne
Multi	ECDHE_RSA_RC4_128_SHA256	TLS 1.2	C011	Ne
Vše	TLS_RSA_WITH_NULL_SHA256	TLS 1.2	003B	Ne
ALW	ECDHE_ECDSA_NULL_SHA256	TLS 1.2	C006	Ne
Multi	ECDHE_RSA_NULL_SHA256	TLS 1.2	C010	Ne
ALW	TLS_RSA_WITH_NULL_NULL	TLS 1.2	0000	Ne
ALW z/OS	TLS_RSA_WITH_AES_256_CBC_SHA	TLS 1.0	0035	Ne

Tabulka 78. Pořadí CipherSpecs od IBM MQ 9.2.0 (pokračování)				
Platforma	**CipherSpec**	**Protokol**	**Hexadecimální kód**	**Standardně povoleno**
ALW z/OS	TLS_RSA_WITH_AES_128_CBC_SHA	TLS 1.0	002F	Ne
IBM i	AES_SHA_US	TLS 1.0	002E	Ne
Vše	TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS 1.0	000A	Ne
Vše	TLS_RSA_WITH_RC4_128_SHA	TLS 1.0	0005	Ne
IBM i	TLS_RSA_WITH_RC4_128_MD5	TLS 1.0	0004	Ne
Vše	TLS_RSA_WITH_DES_CBC_SHA	TLS 1.0	0005	Ne
IBM i	TLS_RSA_EXPORT_WITH_RC4_40_MD5	TLS 1.0	0003	Ne
IBM i	TLS_RSA_EXPORT_WITH_RC2_40_MD5	TLS 1.0	0006	Ne
IBM i	TLS_RSA_WITH_NULL_SHA	TLS 1.0	0002	Ne
IBM i	TLS_RSA_WITH_NULL_MD5	TLS 1.0	0001	Ne
Vše	TRIPLE_DES_SHA_US	SSL v3	000A	Ne
Vše	RC4_SHA_US	SSL v3	0005	Ne
Vše	RC4_MD5_US	SSL v3	0004	Ne
Vše	DES_SHA_EXPORT	SSL v3	0005	Ne
Vše	RC4_MD5_EXPORT	SSL v3	0003	Ne
Vše	RC2_MD5_EXPORT	SSL v3	0006	Ne
Vše	NULL_SHA	SSL v3	0002	Ne
Vše	NULL_MD5	SSL v3	0001	Ne
ALW	FIPS_WITH_3DES_EDE_CBC_SHA	SSL v3	FEFF	Ne
ALW	RC4_56_SHA_EXPORT1024	SSL v3	0064	Ne
ALW	DES_SHA_EXPORT1024	SSL v3	0062	Ne

Tabulka 78. Pořadí CipherSpecs od IBM MQ 9.2.0 (pokračování)				
Platforma	**CipherSpec**	**Protokol**	**Hexadecimální kód**	**Standardně povoleno**
ALW	FIPS_WITH_DES_CBC_SHA	SSL v3	FEFE	Ne

Tento seznam byl vytvořen uspořádáním protokolů s výchozím seznamem poskytnutým šifrovací knihovnou používanou produktem IBM MQ v systému z/OS a je konzistentní v rámci produktu z/OS a distribuovaných platforem.

změna pořadí

Pokud požadujete jiné pořadí, můžete zadat nové pořadí specifikací CipherSpecs pomocí atributu **AllowedCipherSpecs** sekce SSL na systému IBM MQ for Multiplatforms z/OS nebo sekce TransportSecurity na systému IBM MQ for z/OS, s následujícími pravidly:

- Vyšší verze protokolu se používají vždy bez ohledu na jejich umístění v seznamu.
- Všechny zakázané specifikace CipherSpecs jsou znovu povoleny, pokud jsou uvedeny v seznamu.
- Pořadí seznamu serveru TLS má vyšší prioritu než klient TLS.
- Je-li povoleno zabezpečení TLS 1.3 , některé specifikace CipherSpecs nejsou podporovány.

Například v systému IBM MQ for Multiplatforms, pokud je ve správci front nakonfigurováno následující:

```
SSL:
AllowedCipherSpecs=TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_AES_128_GCM_SHA256,
TLS_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_256_CBC_SHA
```

z/OS a v systému IBM MQ for z/OS, pokud je ve správci front nakonfigurováno následující:

```
TransportSecurity:
AllowedCipherSpecs=TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_AES_128_GCM_SHA256,
TLS_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_256_CBC_SHA
```

pak:

- Klient připojující se pomocí ANY_TLS12 bude pravděpodobně používat protokol TLS 1.2 CipherSpec TLS_RSA_WITH_AES_128_GCM_SHA256.
- Klient připojující se pomocí příkazu ANY_TLS12_OR_HIGHER bude pravděpodobně používat protokol TLS 1.3 CipherSpec TLS_AES_128_GCM_SHA256 (za předpokladu, že klient podporuje protokol TLS 1.3).
- Klient, který se připojuje pomocí protokolu TLS 1.0 CipherSpec TLS_RSA_WITH_AES_256_CBC_SHA použije tuto specifikaci CipherSpec.

Předchozí verze produktu IBM MQ

Před produktem IBM MQ 9.2.0bylo použito následující pořadí CipherSpecs :

Tabulka 79. CipherSpecs objednat před IBM MQ 9.2.0			
Platforma	**CipherSpec**	**Protokol**	**Standardně povoleno**
ALW z/OS	TLS_RSA_WITH_AES_128_CBC_SHA	TLS 1.0	Ne
IBM i	AES_SHA_US	TLS 1.0	Ne

Tabulka 79. CipherSpecs objednat před IBM MQ 9.2.0 (pokračování)			
Platforma	**CipherSpec**	**Protokol**	**Standardně povoleno**
ALW z/OS	TLS_RSA_WITH_AES_256_CBC_SHA	TLS 1.0	Ne
Vše	RC4_SHA_US	SSL v3	Ne
Vše	TLS_RSA_WITH_RC4_128_SHA	TLS 1.0	Ne
Vše	RC4_MD5_US	SSL v3	Ne
IBM i	TLS_RSA_WITH_RC4_128_MD5	TLS 1.0	Ne
Vše	TRIPLE_DES_SHA_US	SSL v3	Ne
Vše	TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS 1.0	Ne
ALW	DES_SHA_EXPORT1024	SSL v3	Ne
Vše	RC4_56_SHA_EXPORT1024	SSL v3	Ne
Vše	RC4_MD5_EXPORT	SSL v3	Ne
IBM i	TLS_RSA_EXPORT_WITH_RC4_40_MD5	TLS 1.0	Ne
Vše	RC2_MD5_EXPORT	SSL v3	Ne
IBM i	TLS_RSA_EXPORT_WITH_RC2_40_MD5	TLS 1.0	Ne
Vše	DES_SHA_EXPORT	SSL v3	Ne
Vše	TLS_RSA_WITH_DES_CBC_SHA	TLS 1.0	Ne
Vše	NULL_SHA	SSL v3	Ne
IBM i	TLS_RSA_WITH_NULL_SHA	TLS 1.0	Ne
Vše	NULL_MD5	SSL v3	Ne
IBM i	TLS_RSA_WITH_NULL_MD5	TLS 1.0	Ne
ALW	FIPS_WITH_DES_CBC_SHA	SSL v3	Ne
ALW	FIPS_WITH_3DES_EDE_CBC_SHA	SSL v3	Ne
Vše	TLS_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2	Ano
Vše	TLS_RSA_WITH_AES_256_CBC_SHA256	TLS 1.2	Ano

Tabulka 79. CipherSpecs objednat před IBM MQ 9.2.0 (pokračování)			
Platforma	**CipherSpec**	**Protokol**	**Standardně povoleno**
Vše	TLS_RSA_WITH_NULL_SHA256	TLS 1.2	Ne
Vše	TLS_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2	Ano
Vše	TLS_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2	Ano
ALW	ECDHE_ECDSA_RC4_128_SHA256	TLS 1.2	Ne
ALW	ECDHE_ECDSA_3DES_EDE_CBC_SHA256	TLS 1.2	Ne
Multi	ECDHE_RSA_RC4_128_SHA256	TLS 1.2	Ne
Multi	ECDHE_RSA_3DES_EDE_CBC_SHA256	TLS 1.2	Ne
Vše	ECDHE_ECDSA_AES_128_CBC_SHA256	TLS 1.2	Ano
Vše	ECDHE_ECDSA_AES_256_CBC_SHA384	TLS 1.2	Ano
Vše	ECDHE_RSA_AES_128_CBC_SHA256	TLS 1.2	Ano
Vše	ECDHE_RSA_AES_256_CBC_SHA384	TLS 1.2	Ano
Multi	ECDHE_ECDSA_AES_128_GCM_SHA256	TLS 1.2	Ano
Multi	ECDHE_ECDSA_AES_256_GCM_SHA384	TLS 1.2	Ano
Vše	ECDHE_RSA_AES_128_GCM_SHA256	TLS 1.2	Ano
Vše	ECDHE_RSA_AES_256_GCM_SHA384	TLS 1.2	Ano
Multi	ECDHE_RSA_NULL_SHA256	TLS 1.2	Ne
ALW	ECDHE_ECDSA_NULL_SHA256	TLS 1.2	Ne
ALW	TLS_RSA_WITH_NULL_NULL	TLS 1.2	Ne
ALW	TLS_RSA_WITH_RC4_128_SHA256	TLS 1.2	Ne
Multi	TLS_AES_128_GCM_SHA256	TLS 1.3	Ano
Multi	TLS_AES_256_GCM_SHA384	TLS 1.3	Ano

Tabulka 79. CipherSpecs objednat před IBM MQ 9.2.0 (pokračování)			
Platforma	**CipherSpec**	**Protokol**	**Standardně povoleno**
Multi	TLS_CHACHA20_POLY1305_SHA256	TLS 1.3	Ano
ALW	TLS_AES_128_CCM_SHA256	TLS 1.3	Ano
ALW	TLS_AES_128_CCM_8_SHA256	TLS 1.3	Ano

Důležité: Od 23rd července 2020 následující atribut AllowedCipherSpecs povoluje pouze CipherSpecs , které jsou momentálně standardně povoleny. Měli byste však ověřit specifikace CipherSpecs povolené následujícím atributem AllowedCiphers aktuálními daty, abyste se ujistili, že specifikace CipherSpecs , které byly od tohoto data zamítnuty, nejsou neúmyslně znovu povoleny.

Potřebujete-li se vrátit do tohoto pořadí specifikací CipherSpecs, můžete tak učinit pomocí následující hodnoty atributu sekce **AllowedCipherSpecs** SSL/TransportSecurity :

```
AllowedCipherSpecs=TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384,ECDHE_ECDSA_AES_128_CBC_SHA256,
ECDHE_ECDSA_AES_256_CBC_SHA384,ECDHE_RSA_AES_128_CBC_SHA256,ECDHE_RSA_AES_256_CBC_SHA384,
ECDHE_ECDSA_AES_128_GCM_SHA256,ECDHE_ECDSA_AES_256_GCM_SHA384,ECDHE_RSA_AES_128_GCM_SHA256,
ECDHE_RSA_AES_256_GCM_SHA384
```

Poskytnutí vlastního seznamu seřazených a povolených CipherSpecs na systému IBM MQ for Multiplatforms

Multi

Můžete poskytnout alternativní sadu CipherSpecs , která je povolena, a v pořadí podle předvolby, pro použití s kanály IBM MQ , buď pomocí atributu ALW proměnná prostředí **AMQ_ALLOWED_CIPHERS** , nebo pomocí atributu **AllowedCipherSpecs** sekce SSL souboru `.ini` . Toto nastavení můžete použít z jedné z následujících příčin:

- Chcete-li zakázat modulům listener IBM MQ přijímat příchozí požadavky na spuštění kanálu, pokud nepoužívají jednu z uvedených specifikací CipherSpecs.
- Chcete-li změnit pořadí priority CipherSpecs , které se používají v navázání komunikace TLS.

Tuto funkci lze použít k řízení CipherSpecs , které jsou součástí specifikace ANY* CipherSpecs.

Atribut sekce SSL proměnné prostředí **AMQ_ALLOWED_CIPHERS** nebo **AllowedCipherSpecs** přijímá:

- Jeden název CipherSpec .
- Čárkami oddělený seznam názvů CipherSpec , které chcete znovu povolit.
- Speciální hodnota ALLpředstavující všechny CipherSpecs.

Poznámka: Neměli byste povolovat specifikace **ALL** CipherSpecs, protože tím povolíte protokoly SSL 3.0 a TLS 1.0 a velký počet slabých šifrovacích algoritmů.

Je-li toto nastavení nakonfigurováno, přepíše výchozí seznam CipherSpec a způsobí, že IBM MQ bude ignorovat slabá nastavení zamítnutí šifer (viz níže):

- IBM MQ listenery přijímají pouze návrhy SSL/TLS, které používají jednu z uvedených CipherSpecs.
- Kanály IBM MQ povolují pouze prázdnou hodnotu SSLCIPH nebo jednu z pojmenovaných CipherSpecs.
- **runmqsc** dokončení tabulátoru hodnot SSLCIPH omezuje hodnoty dokončení na jeden z názvů CipherSpecs.

Chcete-li například povolit pouze definování/změnu kanálů a přijetí modulu listener ECDHE_RSA_AES_128_GCM_SHA256 nebo ECDHE_ECDSA_AES_256_GCM_SHA384 , můžete v souboru `qm.ini` nastavit následující:

```
SSL:
  AllowedCipherSpecs=ECDHE_RSA_AES_128_GCM_SHA256, ECDHE_ECDSA_AES_256_GCM_SHA384
```

Dále budou specifikace CipherSpecs v tomto seznamu použity k určení priority CipherSpecs použitých během navázání komunikace TLS. Pokud například uvedete seznam `TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA256` , je pravděpodobné, že během navázání komunikace bude vybrána volba TLS_RSA_WITH_AES_128_CBC_SHA256 CipherSpec přes TLS_RSA_WITH_AES_256_CBC_SHA256 CipherSpec , pokud se klient připojí a uvede obě tyto CipherSpecs, tj. klienta připojujícího se pomocí ANY_TLS12.

Všimněte si, že šifry používané kanály AMQP nebo MQTT lze omezit pomocí nastavení souboru java.security .

Poskytnutí vlastního seznamu seřazených a povolených CipherSpecs na systému IBM MQ for z/OS

Můžete poskytnout alternativní sadu specifikací CipherSpecs , které jsou povoleny, a v upřednostňovaném pořadí, pro použití s kanály IBM MQ , pomocí atributu sekce **AllowedCipherSpecs** TransportSecurity Datová sada QMINI. Možná to budete chtít provést z jedné z následujících příčin:

- Chcete-li zakázat modulům listener IBM MQ přijímat příchozí požadavky na spuštění kanálu, pokud nepoužívají jednu z uvedených specifikací CipherSpecs.
- Chcete-li změnit pořadí priority CipherSpecs , které se používají v navázání komunikace TLS.

Tuto funkci můžete použít k řízení CipherSpecs , které jsou součástí specifikace ANY* CipherSpecs. Atribut **AllowedCipherSpecs** přijímá:

- Jeden název CipherSpec .
- Čárkami oddělený seznam názvů CipherSpec , které chcete znovu povolit.
- Speciální hodnota ALLpředstavující všechny CipherSpecs.

  Poznámka: Neměli byste povolovat specifikace **ALL** CipherSpecs, protože tím povolíte protokoly SSL 3.0 a TLS 1.0 a velký počet slabých šifrovacích algoritmů. Pokud toto nastavení nakonfigurujete, přepíše výchozí seznam CipherSpec a způsobí, že IBM MQ bude ignorovat slabá nastavení šifrování; viz “Povolení zamítnutých specifikací CipherSpecs na systému z/OS” na stránce 457.

Moduly listener produktu IBM MQ přijímají pouze návrhy SSL/TLS, které používají jednu z uvedených specifikací CipherSpecs a IBM MQ umožňují pouze prázdnou hodnotu SSLCIPH nebo jednu z uvedených specifikací CipherSpecs.

Chcete-li například povolit pouze definování/změnu kanálů a přijetí modulu listener ECDHE_RSA_AES_128_GCM_SHA256 nebo ECDHE_RSA_AES_256_GCM_SHA384 , můžete nastavit následující:

```
TransportSecurity:
  AllowedCipherSpecs=ECDHE_RSA_AES_128_GCM_SHA256,
                     ECDHE_RSA_AES_256_GCM_SHA384
```

Dále se CipherSpecs v tomto seznamu používají k určení priority CipherSpecs používaných během navázání komunikace TLS. Pokud například uvedete seznam TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA256 je pravděpodobné, že během navázání komunikace bude TLS_RSA_WITH_AES_128_CBC_SHA256 CipherSpec vybrán přes TLS_RSA_WITH_AES_256_CBC_SHA256 CipherSpec , pokud se klient připojí a uvede oba tyto CipherSpecs, tedy klienta, který se připojí pomocí ANY_TLS12.

Deprecated Zamítnuté specifikace CipherSpecs

Seznam zamítnutých specifikací CipherSpecs , které můžete v případě potřeby použít s produktem IBM MQ .

Poznámka: V systému AIX, Linux, and Windowsposkytuje produkt IBM MQ kompatibilitu se standardem FIPS 140-2 prostřednictvím šifrovacího modulu IBM Crypto for C (ICC) . Certifikát pro tento modul byl přesunut do historického stavu. Zákazníci by si měli prohlédnout IBM Crypto for C (ICC) certifikát a měli by si být vědomi všech doporučení poskytnutých NIST. Náhradní modul FIPS 140-3 momentálně probíhá a jeho stav lze zobrazit jeho vyhledáním v modulech NIST CMVP v seznamu procesů.

Informace o povolení zamítnutých specifikací CipherSpecsviz “Povolení zamítnutých specifikací CipherSpecs na systému IBM MQ for Multiplatforms” na stránce 456 nebo “Povolení zamítnutých specifikací CipherSpecs na systému z/OS” na stránce 457.

Zamítnuté specifikace CipherSpecs , které můžete použít s podporou protokolu IBM MQ TLS, jsou uvedeny v následující tabulce.

Tabulka 80. Zamítnuté specifikace CipherSpecs můžete znovu povolit pro použití s produktem IBM MQ.

Podpora platformy “1” na stránce 456	Název specifikace šifrování	Hexadecimální kód	Použitý protokol	Integrita dat	Šifrovací algoritmus (šifrovací bity)	FIPS “2” na stránce 456	Suite B	Aktualizovat při zamítnutí
CipherSpecs pro SSL 3.0								
IBM i	AES_SHA_US “3” na stránce 456	002F	SSL 3.0	SHA-1	AES (128)	Ne	Ne	9.0.0.0
Vše	DES_SHA_EXPORT “3” na stránce 456 “4” na stránce 456 “5” na stránce 456	0005	SSL 3.0	SHA-1	DES (56)	Ne	Ne	9.0.0.0
ALW	DES_SHA_EXPORT1024 “3” na stránce 456 “6” na stránce 456	0062	SSL 3.0	SHA-1	DES (56)	Ne	Ne	9.0.0.0
ALW	FIPS_WITH_DES_CBC_SHA “3” na stránce 456	FEFE	SSL 3.0	SHA-1	DES (56)	Ne“7” na stránce 456	Ne	9.0.0.0
ALW	FIPS_WITH_3DES_EDE_CBC_SHA “3” na stránce 456	FEFF	SSL 3.0	SHA-1	3DES (168)	Ne“8” na stránce 456	Ne	9.0.0.1 a 9.0.1
Vše	NULL_MD5 “3” na stránce 456	0001	SSL 3.0	MD5	Není	Ne	Ne	9.0.0.1
Vše	NULL_SHA “3” na stránce 456	0002	SSL 3.0	SHA-1	Není	Ne	Ne	9.0.0.1
Vše	RC2_MD5_EXPORT “3” na stránce 456 “4” na stránce 456 “5” na stránce 456	0006	SSL 3.0	MD5	RC2 (40)	Ne	Ne	9.0.0.0
Vše	RC4_MD5_EXPORT “4” na stránce 456 “3” na stránce 456	0003	SSL 3.0	MD5	RC4 (40)	Ne	Ne	9.0.0.0
Vše	RC4_MD5_US “3” na stránce 456	0004	SSL 3.0	MD5	RC4 (128)	Ne	Ne	9.0.0.0
Vše	RC4_SHA_US “3” na stránce 456 “5” na stránce 456	0005	SSL 3.0	SHA-1	RC4 (128)	Ne	Ne	9.0.0.0

Tabulka 80. Zamítnuté specifikace CipherSpecs můžete znovu povolit pro použití s produktem IBM MQ. (pokračování)

Podpora platformy "1" na stránce 456	Název specifikace šifrování	Hexadecimální kód	Použitý protokol	Integrita dat	Šifrovací algoritmus (šifrovací bity)	FIPS "2" na stránce 456	Suite B	Aktualizovat při zamítnutí
ALW	RC4_56_SHA_EXPORT1024 "3" na stránce 456 "6" na stránce 456	0064	SSL 3.0	SHA-1	RC4 (56)	Ne	Ne	9.0.0.0
Vše	TRIPLE_DES_SHA_US "3" na stránce 456 "5" na stránce 456	000A	SSL 3.0	SHA-1	3DES (168)	Ne	Ne	9.0.0.1 a 9.0.1
CipherSpecs pro TLS 1.0								
IBM i	TLS_RSA_EXPORT_WITH_RC2_40_MD5 "3" na stránce 456	0006	TLS 1.0	MD5	RC2 (40)	Ne	Ne	9.0.0.0
IBM i	TLS_RSA_EXPORT_WITH_RC4_40_MD5 "3" na stránce 456 "4" na stránce 456	0003	TLS 1.0	MD5	RC4 (40)	Ne	Ne	9.0.0.0
Vše	TLS_RSA_WITH_DES_CBC_SHA "3" na stránce 456	0005	TLS 1.0	SHA-1	DES (56)	Ne "9" na stránce 456	Ne	9.0.0.0
IBM i	TLS_RSA_WITH_NULL_MD5 "3" na stránce 456	0001	TLS 1.0	MD5	Není	Ne	Ne	9.0.0.1
IBM i	TLS_RSA_WITH_NULL_SHA "3" na stránce 456	0002	TLS 1.0	SHA-1	Není	Ne	Ne	9.0.0.1
IBM i	TLS_RSA_WITH_RC4_128_MD5 "3" na stránce 456	0004	TLS 1.0	MD5	RC4 (128)	Ne	Ne	9.0.0.0
z/OS ALW	TLS_RSA_WITH_AES_128_CBC_SHA "10" na stránce 456	002F	TLS 1.0	SHA-1	AES (128)	Ano	Ne	9.0.5
z/OS ALW	TLS_RSA_WITH_AES_256_CBC_SHA "6" na stránce 456 "10" na stránce 456	0035	TLS 1.0	SHA-1	AES (256)	Ano	Ne	9.0.5
Vše	TLS_RSA_WITH_3DES_EDE_CBC_SHA	000A	TLS 1.0	SHA-1	3DES (168)	Ano	Ne	9.0.0.1 a 9.0.1
CipherSpecs pro TLS 1.2								
ALW	ECDHE_ECDSA_NULL_SHA256 "3" na stránce 456	C006	TLS 1.2	SHA-1	Není	Ne	Ne	9.0.0.1
ALW	ECDHE_ECDSA_RC4_128_SHA256 "3" na stránce 456	C007	TLS 1.2	SHA-1	RC4 (128)	Ne	Ne	9.0.0.0
ALW IBM i	ECDHE_RSA_NULL_SHA256 "3" na stránce 456	C010	TLS 1.2	SHA-1	Není	Ne	Ne	9.0.0.1
ALW IBM i	ECDHE_RSA_RC4_128_SHA256 "3" na stránce 456	C011	TLS 1.2	SHA-1	RC4 (128)	Ne	Ne	9.0.0.0

Tabulka 80. Zamítnuté specifikace CipherSpecs můžete znovu povolit pro použití s produktem IBM MQ. (pokračování)

Podpora platformy "1" na stránce 456	Název specifikace šifrování	Hexadecimální kód	Použitý protokol	Integrita dat	Šifrovací algoritmus (šifrovací bity)	FIPS "2" na stránce 456	Suite B	Aktualizovat při zamítnutí
ALW	TLS_RSA_WITH_NULL_NULL "3" na stránce 456	0000	TLS 1.2	Není	Není	Ne	Ne	9.0.0.1
Vše	TLS_RSA_WITH_NULL_SHA256 "3" na stránce 456	003B	TLS 1.2	SHA-256	Není	Ne	Ne	9.0.0.1
ALW	TLS_RSA_WITH_RC4_128_SHA256 "3" na stránce 456	0005	TLS 1.2	SHA-1	RC4 (128)	Ne	Ne	9.0.0.0
ALW	ECDHE_ECDSA_3DES_EDE_CBC_SHA256	C0008	TLS 1.2	SHA-1	3DES (168)	Ano	Ne	9.0.0.1 a 9.0.1
ALW IBM i	ECDHE_RSA_3DES_EDE_CBC_SHA256	C012	TLS 1.2	SHA-1	3DES (168)	Ano	Ne	9.0.0.1 a 9.0.1

Tabulka 80. Zamítnuté specifikace CipherSpecs můžete znovu povolit pro použití s produktem IBM MQ. (pokračování)

Podpora platformy "1" na stránce 456	Název specifikace šifrování	Hexadecimální kód	Použitý protokol	Integrita dat	Šifrovací algoritmus (šifrovací bity)	FIPS "2" na stránce 456	Suite B	Aktualizovat při zamítnutí

Notes:

1. Seznam platforem pokrytých každou ikonou platformy naleznete v tématu Ikony použité v dokumentaci k produktu.
2. Uvádí, zda má specifikace šifrování certifikaci FIPS na platformě s certifikací FIPS. Vysvětlení FIPS viz Federal Information Processing Standards (FIPS).
3. ALW Tyto specifikace CipherSpecs jsou zakázány, je-li povolen protokol TLS 1.3 (prostřednictvím vlastnosti AllowTLSV13 v `qm.ini`).

   z/OS Správci front vytvoření v IBM MQ for z/OS 9.2.0 nebo novější standardně povolují protokol TLS 1.3, který zakazuje tyto specifikace CipherSpecs. Tyto specifikace CipherSpecs můžete povolit, je-li to nutné, vypnutím protokolu TLS V1.3. To provedete přidáním hodnoty **AllowTLSV13**=*FALSE* do sekce TransportSecurity datové sady QMINI v JCL správce front. Správci front migrovaní do verze IBM MQ for z/OS 9.2.0 ze starší verze nemají standardně povoleny TLS 1.3, a proto mají tyto specifikace CipherSpecs povoleny.
4. Maximální velikost klíče pro navázání komunikace je 512 bitů. Pokud některý z certifikátů, vyměněných během navázání komunikace SSL, bude mít velikost klíče větší než 512 bitů, vygeneruje se dočasný 512 bitový klíč určený pro navázání komunikace.
5. Tyto specifikace šifrování již produkt IBM MQ classes for Java nebo IBM MQ classes for JMS nepodporuje. Další informace viz Specifikace šifrování a šifrovací sady SSL/TLS v produktu IBM MQ classes for Java nebo Specifikace šifrování a šifrovací sady SSL/TLS v produktu IBM MQ classes for JMS.
6. Velikost klíče pro navázání komunikace je 1024 bitů.
7. Deprecated Tato specifikace šifrování byla certifikována FIPS 140-2 před 19. květnem 2007. Název `FIPS_WITH_DES_CBC_SHA` je historický a odráží skutečnost, že tato specifikace CipherSpec dříve byla kompatibilní se standardem FIPS (ale již není). Tato specifikace šifrování byla zamítnuta a její použití se nedoporučuje.
8. Deprecated Název `FIPS_WITH_3DES_EDE_CBC_SHA` je historický a odráží skutečnost, že tato specifikace CipherSpec dříve byla kompatibilní se standardem FIPS (ale již není). Použití této specifikace šifrování bylo zamítnuto.
9. Tato specifikace šifrování byla certifikována FIPS 140-2 před 19. květnem 2007.
10. z/OS Opětovné povolení pouze těchto specifikací CipherSpec nevyžaduje použití příkazu CSQXWEAK DD.

Povolení zamítnutých specifikací CipherSpecs na systému IBM MQ for Multiplatforms

Multi

Při výchozím nastavení není v definici kanálu povoleno určit zamítnutou specifikaci CipherSpec . Pokusíte-li se zadat zamítnutou specifikaci CipherSpec v systému IBM MQ for Multiplatforms, obdržíte zprávu AMQ8242: Definice SSLCIPH je chybná a funkce PCF vrátí hodnotu `MQRCCF_SSL_CIPHER_SPEC_ERROR`.

Kanál se zamítnutou specifikací CipherSpecnelze spustit. Pokud se o to pokusíte se zamítnutou specifikací CipherSpec, systém vrátí klientovi hodnotu `MQCC_FAILED (2)` spolu s hodnotou **Reason** `MQRC_SSL_INITIALIZATION_ERROR (2393)`.

Můžete znovu povolit jednu nebo více zamítnutých specifikací CipherSpecs pro definování kanálů za běhu na serveru nastavením proměnné prostředí **AMQ_SSL_WEAK_CIPHER_ENABLE**.

Proměnná prostředí **AMQ_SSL_WEAK_CIPHER_ENABLE** přijímá:

- jeden název CipherSpec nebo
- Čárkami oddělený seznam názvů CipherSpec , které chcete znovu povolit, nebo
- Speciální hodnota `ALL`představující všechny CipherSpecs.

Upozornění: Ačkoli volba `ALL` je platná, měli byste ji používat **pouze** ve specifické situaci, kterou vyžaduje váš podnik, jako opětné povolení `ALL` CipherSpecs povoluje protokoly SSL 3.0 a TLS 1.0 , stejně jako velký počet slabých šifrovacích algoritmů.

Chcete-li například znovu povolit ECDHE_RSA_RC4_128_SHA256, nastavte tuto proměnnou prostředí:

```
export AMQ_SSL_WEAK_CIPHER_ENABLE=ECDHE_RSA_RC4_128_SHA256
```

nebo případně změňte sekci SSL v souboru `qm.ini` nastavením:

```
SSL:
  AllowTLSV1=Y
  AllowWeakCipherSpec=ECDHE_RSA_RC4_128_SHA256
```

Povolení zamítnutých specifikací CipherSpecs na systému z/OS

z/OS

Při výchozím nastavení není v definici kanálu povoleno určit zamítnutou specifikaci CipherSpec . Pokud se pokusíte určit zamítnutou specifikaci CipherSpec v systému z/OS, obdržíte zprávu CSQM102E, zprávu CSQX616Enebo zprávu CSQX674E.

Pokud obdržíte některou z těchto zpráv, postupujte podle pokynů uvedených v této části a váš podnik musí znovu povolit používání slabých CipherSpecs.

Upozornění: Aby se v následujících pokynech projevily příkazy fiktivní definice (DD), musí mít parametr SSLTASKS nenulovou hodnotu. Pokud to vyžaduje změnu SSLTASKS, musíte restartovat inicializátor kanálu.

V systému IBM MQ for z/OSje aktuální metoda řízení slabých nebo poškozených CipherSpecs následující:

- Chcete-li znovu povolit použití slabých specifikací CipherSpecs, proveďte to přidáním příkazu definice fiktivních dat (DD) s názvem `CSQXWEAK` do kódu JCL inicializátoru kanálu. Je-li tato volba zadána samostatně, povoluje pouze slabé CipherSpecs přidružené k protokolu TLS 1.2 ; například:

  ```
  //CSQXWEAK DD DUMMY
  ```

  Poznámka: Ne všechny zamítnuté specifikace CipherSpecs vyžadují použití tohoto příkazu DD, viz poznámka 10 v předchozí tabulce.
- Chcete-li znovu povolit použití volby SSLv3 CipherSpecs, můžete tak učinit také přidáním fiktivního příkazu DD s názvem `CSQXSSL3` do kódu JCL inicializátoru kanálu. Všechny specifikace SSLv3 CipherSpecs jsou považovány za **slabé**, takže musíte také zadat `CSQXWEAK`:

  ```
  //CSQXSSL3 DD DUMMY
  ```

- Chcete-li znovu povolit zamítnuté specifikace TLS V1 CipherSpecs, přidejte do kódu JCL inicializátoru kanálu fiktivní příkaz DD s názvem TLS10ON (zapněte protokol TLS V1.0). Je-li zadán samostatně, povolí silné CipherSpecs přidružené k protokolu TLS 1.0 :

  ```
  //TLS10ON DD DUMMY
  ```

  Je-li uvedeno s parametrem CSQXWEAK , povolí také **slabé** CipherSpecs přidružené k protokolu TLS 1.0.
- Chcete-li explicitně vypnout zamítnuté specifikace TLS V1 CipherSpecs, proveďte to přidáním fiktivního příkazu DD s názvem TLS10OFF (turn TLS V1.0 OFF) do JCL inicializátoru kanálu; například:

  ```
  //TLS10OFF DD DUMMY
  ```

Chcete-li vyjednávat pouze s listenerem pomocí specifikací šifer uvedených ve výchozím seznamu specifikací šifer **System SSL** , musíte definovat následující příkaz DD v JCL CHINIT:

```
JCL: //GSKDCIPS DD DUMMY
```

Důležité: Pro systém IBM MQ for z/OS 9.2.0 a novější jsou dříve uvedené karty DD a hodnota **AllowTLSV13** brány v úvahu při zobrazování zpráv během spuštění inicializátoru kanálu, aby se označilo, které protokoly jsou povoleny a které ne. Takže i když je uvedena jedna z dříve uvedených karet DD, může to znamenat, že kvůli kombinaci těchto nastavení nelze povolit určitý protokol s jiným protokolem. Například protokol SSL 3.0 není povolen, pokud je povolen protokol TLS 1.3 .

Existují alternativní mechanizmy, které lze použít k vynucené opětovnému povolení slabých specifikací CipherSpecs, a podporu SSLv3 , pokud není změna definice dat vhodná. Pro další informace kontaktujte IBM Service.

Související pojmy

“Digitální certifikáty a kompatibilita CipherSpec v produktu IBM MQ” na stránce 46
Toto téma poskytuje informace o tom, jak zvolit příslušné specifikace CipherSpecs a digitální certifikáty pro vaši zásadu zabezpečení, a to nastíněním vztahu mezi specifikacemi CipherSpecs a digitálními certifikáty v produktu IBM MQ.

Související odkazy

Definovat kanál
POZMĚNIT KANÁL

Relace mezi nastaveními aliasu CipherSpec

Tyto informace popisují očekávané chování s různými kombinacemi aliasů CipherSpecs v konfiguracích klienta a serveru. Klient zde odkazuje na entitu, která zahajuje komunikaci, například na klientskou aplikaci nebo kanál odesilatele správce front, a server odkazuje na entitu, která přijímá komunikaci od klienta, například kanál připojení serveru nebo kanál příjemce.

Minimální protokol versus pevný protokol CipherSpecs

Produkt IBM MQ podporuje dva různé typy CipherSpecs:

Minimální protokol
: Minimální specifikace CipherSpecs protokolu jsou ty, které nenastavují horní mez, například ANY, ANY_TLS12_OR_HIGHER nebo ANY_TLS13_OR_HIGHER.

Pevný protokol
: Pevné protokoly CipherSpecs jsou ty, které identifikují specifický protokol, například ANY_TLS12 a ANY_TLS13, nebo specifický algoritmus, například ECDHE_ECDSA_3DES_EDE_CBC_SHA256.

Od verze IBM MQ 9.2.0jsou minimální a pevný protokol CipherSpecs podporovány na všech platformách.

Chcete-li maximalizovat jednoduchost konfigurace při zachování zabezpečení, doporučuje se na obou stranách kanálu používat **minimální protokol** CipherSpecs . To umožňuje, aby vaše komunikace automaticky podporovaly a používaly vyšší verzi protokolu TLS, když obě strany podporují novou verzi bez nutnosti měnit konfiguraci obou stran.

Použití **minimálního protokolu** CipherSpec na straně inicializace, ale **pevný protokol** CipherSpec na straně příjemce může mít za následek odmítnutí připojení a

- Multi Jsou vydávány zprávy AMQ9631 a AMQ9641 .
- z/OS Vydávané zprávy CSQX631E a CSQX641E .

V následujících tabulkách je uveden vztah mezi různými nastaveními aliasu CipherSpec a očekávaným výsledkem. Tabulka 81 na stránce 459 ukazuje očekávané chování, když TLS 1.3 není povoleno buď na klientovi, serveru, nebo na obou. Tabulka 82 na stránce 459 ukazuje očekávané chování při povolení TLS 1.3 na klientovi i na serveru. V obou případech jsou specifikace CipherSpecs pro klienta zobrazeny na ose Y tabulky a specifikace CipherSpecs pro server jsou zobrazeny na ose X tabulky.

Poznámka: V následujících tabulkách buňky označené jako *Pravděpodobné selhání* označují potenciální konflikt při zadání **minimálního protokolu** CipherSpec pro jednu část připojení a specifickou (**pevný protokol**) CipherSpec pro jinou část.

Předpokládejme například, že klient a server jsou nastaveny na použití libovolné CipherSpeca kanál serveru je nastaven na použití specifické CipherSpec:

- Pokud nejsilnější podporovaná CipherSpec pro klienta i server odpovídá specifické CipherSpec nakonfigurované v kanálu, navázání komunikace TLS se úspěšně interpretuje.
- Pokud však existuje silnější CipherSpec , kterou klient i server podporují, pak se navázání komunikace TLS interpretuje tak, že toto používá, i když se neshoduje se specifikací CipherSpec uvedenou v kanálu, a navázání komunikace TLS se nezdaří.

Tabulka 81. Očekávané chování v případě, že protokol TLS 1.3 není povolen na klientu, serveru nebo na obou serverech.

	Server			
Klient	**Specifická specifikace TLS 1.2 CipherSpec**	**ANY**	**ANY_ TLS12**	**ANY_TLS12_ OR_HIGHER**
Specifické TLS 1.2 CipherSpec	Připojení	Připojení	Připojení	Připojení
ANY	*Pravděpodobné selhání*	Připojení	Připojení	Připojení
ANY_ TLS12	*Pravděpodobné selhání*	Připojení	Připojení	Připojení
ANY_TLS12_ OR_HIGHER	*Pravděpodobné selhání*	Připojení	Připojení	Připojení

Tabulka 82. Očekávané chování při povolení TLS 1.3 na klientovi i na serveru

	Server						
Klient	**Specifická specifikace TLS 1.2 CipherSpec**	**Specifická specifikace TLS 1.3 CipherSpec**	**ANY**	**ANY_TLS 12**	**ANY_TLS 13**	**ANY_TLS12_ NEBO_VYŠŠÍ**	**ANY_TLS13_ NEBO_VYŠŠÍ**
Specifické TLS 1.2 CipherSpec	Připojení	**Neúspěšné**	Připojení	Připojení	**Neúspěšné**	Připojení	**Neúspěšné**
Specifické TLS 1.3 CipherSpec	**Neúspěšné**	Připojení	Připojení	**Neúspěšné**	Připojení	Připojení	Připojení

Tabulka 82. Očekávané chování při povolení TLS 1.3 na klientovi i na serveru (pokračování)							
	Server						
Klient	**Specifická specifikace TLS 1.2 CipherSpec**	**Specifická specifikace TLS 1.3 CipherSpec**	**ANY**	**ANY_TLS 12**	**ANY_TLS 13**	**ANY_TLS12_ NEBO_VYŠŠÍ**	**ANY_TLS13_ NEBO_VYŠŠÍ**
ANY	**Neúspěšné**	*Pravděpodobné selhání*	Připojení	**Neúspěšné**	Připojení	Připojení	Připojení
ANY_TLS12	*Pravděpodobné selhání*	**Neúspěšné**	Připojení	Připojení	**Neúspěšné**	Připojení	**Neúspěšné**
ANY_TLS13	**Neúspěšné**	*Pravděpodobné selhání*	Připojení	**Neúspěšné**	Připojení	Připojení	Připojení
ANY_TLS12_ OR_HIGHER	**Neúspěšné**	*Pravděpodobné selhání*	Připojení	**Neúspěšné**	Připojení	Připojení	Připojení
ANY_TLS13_ OR_HIGHER	**Neúspěšné**	*Pravděpodobné selhání*	Připojení	**Neúspěšné**	Připojení	Připojení	Připojení

Související pojmy

“Digitální certifikáty a kompatibilita CipherSpec v produktu IBM MQ” na stránce 46
Toto téma poskytuje informace o tom, jak zvolit příslušné specifikace CipherSpecs a digitální certifikáty pro vaši zásadu zabezpečení, a to nastíněním vztahu mezi specifikacemi CipherSpecs a digitálními certifikáty v produktu IBM MQ.

“CipherSpecs a CipherSuites” na stránce 21
Šifrovací bezpečnostní protokoly se musí dohodnout na algoritmech používaných zabezpečeným připojením. CipherSpecs a CipherSuites definují specifické kombinace algoritmů.

“Povolení CipherSpecs” na stránce 438
Povolte CipherSpec pomocí parametru **SSLCIPH** v příkazu **DEFINE CHANNEL** nebo **ALTER CHANNEL** MQSC.

Související úlohy

Migrace existujících konfigurací zabezpečení pro použití ANY_TLS12_OR_HIGHER CipherSpec

Získání informací o specifikacích CipherSpecs pomocí IBM MQ Explorer

Pomocí produktu IBM MQ Explorer můžete zobrazit popisy CipherSpecs.

Chcete-li získat informace o CipherSpecs v produktu “Povolení CipherSpecs” na stránce 438, postupujte takto:

1. Otevřete produkt IBM MQ Explorer a rozbalte složku **Správci front**.
2. Ujistěte se, že jste spustili správce front.
3. Vyberte správce front, se kterým chcete pracovat, a klepněte na volbu **Kanály**.
4. Klepněte pravým tlačítkem myši na kanál, se kterým chcete pracovat, a vyberte volbu **Vlastnosti**.
5. Vyberte stránku vlastností **SSL** .
6. Vyberte ze seznamu položku CipherSpec , se kterou chcete pracovat. V okně pod seznamem se zobrazí popis.

z/OS IBM i Alternativy pro určení CipherSpecs

Na platformách, kde operační systém poskytuje podporu TLS, může systém podporovat nové specifikace CipherSpecs , které nejsou součástí produktu “Povolení CipherSpecs” na stránce 438.

Můžete zadat novou specifikaci CipherSpec s parametrem SSLCIPH, ale hodnota, kterou zadáte, závisí na vaší platformě. Ve všech případech musí specifikace odpovídat specifikaci TLS CipherSpec , která je platná i podporovaná verzí protokolu TLS, kterou váš systém spouští.

Poznámka: Tento oddíl se nevztahuje na systémy AIX, Linux, and Windows , protože specifikace CipherSpecs jsou dodávány s produktem IBM MQ , takže nové specifikace CipherSpecs nejsou po odeslání k dispozici.

IBM i IBM i

Dvouznakový řetězec představující hexadecimální hodnotu.

Další informace o povolených hodnotách viz bod 3 v části Poznámky k použití v části Nastavit informace o znacích pro zabezpečenou relaci.

Upozornění: V souboru **SSLCIPH**byste neměli zadávat hexadecimální hodnoty šifer, protože není jasné, která hodnota šifry bude použita, a volba, který protokol má být použit, je neurčitá. Použití hexadecimálních šifrovacích hodnot může vést k chybám neshody specifikace CipherSpec.

K určení hodnoty můžete použít buď příkaz **CHGMQMCHL** , nebo příkaz **CRTMQMCHL** , například:

```
CRTMQMCHL CHLNAME(' channel name ') SSLCIPH(' hexadecimal value ')
```

Můžete také použít příkaz **ALTER QMGR** MQSC k nastavení parametru **SSLCIPH** .

z/OS z/OS

Čtyřznakový řetězec představující hexadecimální hodnotu. Hexadecimální kódy odpovídají hodnotám definovaným v protokolu TLS.

Další informace viz Definice šifrovacích sad , kde je seznam všech podporovaných specifikací šifer TLS 1.0, TLS 1.2a TLS 1.3 ve formě 4místných hexadecimálních kódů.

Poznámka: Deprecated Chcete-li použít slabou CipherSpecnebo CipherSpec patřící k zamítnutému protokolu, například SSL V3.0 nebo TLS 1.0, musíte určit příslušnou kartu DD ve spouštěcím kódu JCL inicializátoru kanálu. Další informace viz “Zamítnuté specifikace CipherSpecs” na stránce 453.

Aspekty pro klastry IBM MQ

U klastrů IBM MQ je nejbezpečnější používat názvy CipherSpec v produktu “Povolení CipherSpecs” na stránce 438. Pokud použijete alternativní specifikaci, mějte na paměti, že tato specifikace nemusí být platná na jiných platformách. Další informace jsou uvedeny v tématu “SSL/TLS a klastry” na stránce 499.

Určení CipherSpec pro IBM MQ MQI client

Máte tři volby pro určení CipherSpec pro IBM MQ MQI client.

Tyto volby jsou následující:

- Použití tabulky definic kanálů
- Použití pole SSLCipherSpec ve struktuře MQCD na adrese MQCD_VERSION_7 nebo vyšší při volání MQCONNX.
- Použití Active Directory (na systémech Windows s podporou Active Directory)

Určení CipherSuite pomocí IBM MQ classes for Java a IBM MQ classes for JMS

IBM MQ classes for Java a IBM MQ classes for JMS uveďte CipherSuites odlišně od ostatních platforem.

Informace o zadání CipherSuite s produktem IBM MQ classes for Javanaleznete v tématu Podpora TLS (Transport Layer Security) pro produkt Java .

Informace o zadání CipherSuite s produktem IBM MQ classes for JMSnaleznete v tématu Použití protokolu TLS (Transport Layer Security) s produktem IBM MQ classes for JMS .

Určení CipherSpec pro IBM MQ.NET

Pro produkt IBM MQ.NET můžete zadat CipherSpec buď pomocí třídy MQEnvironment, nebo pomocí parametru MQC.SSL_CIPHER_SPEC_PROPERTY v hašovací tabulce vlastností připojení.

Informace o zadání CipherSpec pro nespravovaného klienta .NET naleznete v tématu Povolení TLS pro nespravovaného .NET klienta .

Informace o určení CipherSpec pro spravovaného klienta .NET naleznete v tématu PodporaCipherSpec pro spravovaného klienta .NET .

z/OS Použití AT-TLS s IBM MQ for z/OS

Protokol AT-TLS (Application Transparent Transport Layer Security) poskytuje podporu protokolu TLS pro aplikace z/OS , aniž by tyto aplikace musely implementovat podporu protokolu TLS, nebo si dokonce uvědomují, že se používá protokol TLS. AT-TLS je k dispozici pouze na webu z/OS.

AT-TLS lze použít se všemi verzemi produktu IBM MQ for z/OS.

Před použitím AT-TLS s produktem IBM MQ for z/OSse ujistěte, že rozumíte použitým “Omezení” na stránce 465 .

Chcete-li použít volbu Application Transparent Transport Layer Security , definujte příkazy zásad obsahující sadu pravidel, která jsou používána produktem z/OS Communications Server při rozhodování, která připojení TCP/IP mají protokol TLS transparentně povolen.

Produkt IBM MQ for z/OS má vlastní implementaci TLS, která vyžaduje, aby kanály měly parametr SSLCIPH nakonfigurovaný s podporovanou CipherSpec.

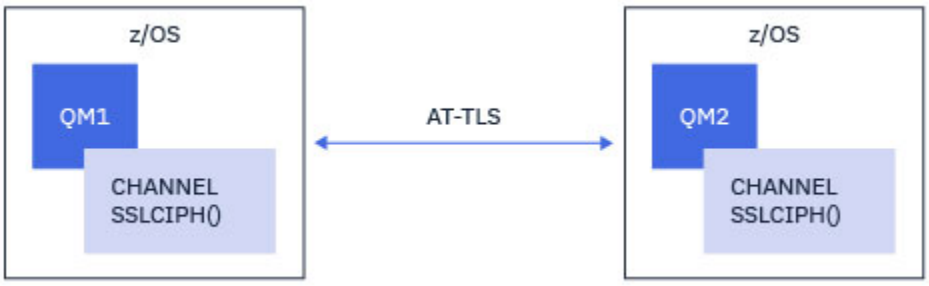
Při rozhodování o povolení protokolu TLS v kanálu může administrátor produktu IBM MQ rozhodnout o použití protokolu AT-TLS nebo IBM MQ TLS. Rozhodnutí se často provádí na základě toho, zda se AT-TLS používá pro jiný middleware, nebo kvůli dopadům na výkon. Základní porovnání výkonu AT-TLS a IBM MQ TLS viz MP16: Plánování a vyladění kapacity pro IBM MQ for z/OS.

Scénáře

Použití AT-TLS s produktem IBM MQ je podporováno v následujících scénářích:

Scénář 1

Mezi dvěma správci front IBM MQ for z/OS , kde obě strany kanálu používají protokol AT-TLS. To znamená, že žádný kanál neurčuje atribut SSLCIPH. Tento přístup lze použít s libovolným kanálem zpráv.



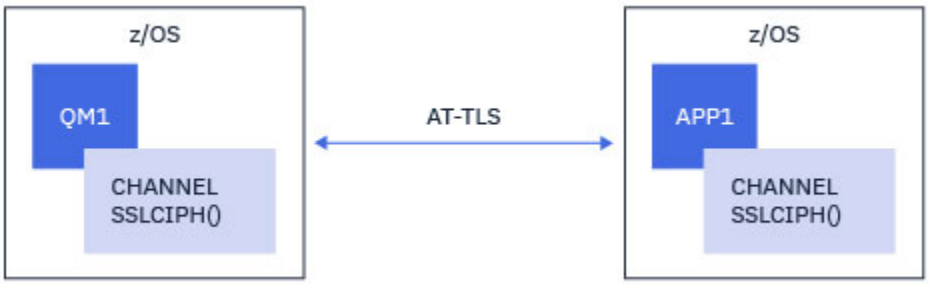
Implementace tohoto scénáře se skládá z definování dvou zásad AT-TLS, jedné pro každou stranu kanálu. Tyto zásady jsou stejné jako ty, které se používají buď s scénáriem 3 , nebo s scénáriem 4.

Pokud například došlo ke změně kanálu z použití jediného kanálu s názvem CipherSpec na kanál AT-TLS, odchozí kanál bude používat zásadu z produktu “Konfigurace AT-TLS v odchozím kanálu pro správce front IBM MQ for Multiplatforms s použitím jednoho názvu s názvem CipherSpec” na stránce 466 a příchozí kanál bude používat zásadu z produktu “Konfigurace AT-TLS v příchozím kanálu ze správce front IBM MQ for Multiplatforms s použitím jediného názvu CipherSpec” na stránce 475.

Pokud byl kanál změněn z použití aliasu CipherSpec na použití AT-TLS, odchozí kanál bude používat zásadu z produktu “Konfigurace AT-TLS v odchozím kanálu pro správce front IBM MQ for Multiplatforms s použitím aliasu CipherSpecs” na stránce 470 a příchozí kanál bude používat zásadu z produktu “Konfigurace AT-TLS v příchozím kanálu ze správce front IBM MQ for Multiplatforms pomocí aliasu CipherSpec” na stránce 479.

Scénář 2

Mezi správcem front systému IBM MQ for z/OS a klientskou aplikací systému IBM MQ Java spuštěnou v systému z/OS , kde obě strany kanálu používají protokol AT-TLS. To znamená, že ani kanál připojení serveru, ani kanál připojení klienta neurčují atribut SSLCIPH.



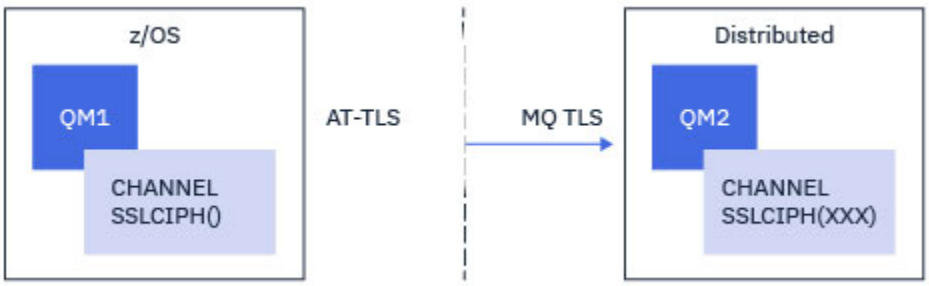
Implementace tohoto scénáře se skládá z definování dvou zásad AT-TLS, jedné pro každou stranu kanálu. Tyto zásady jsou stejné jako ty, které se používají buď s scénáriem 3 , nebo s scénáriem 4.

Pokud například došlo ke změně kanálu z použití jediného kanálu s názvem CipherSpec na kanál AT-TLS, bude kanál připojení klienta používat zásadu z produktu “Konfigurace AT-TLS v odchozím kanálu pro správce front IBM MQ for Multiplatforms s použitím jednoho názvu s názvem CipherSpec” na stránce 466 a kanál připojení serveru bude používat zásadu z produktu “Konfigurace AT-TLS v příchozím kanálu ze správce front IBM MQ for Multiplatforms s použitím jediného názvu CipherSpec” na stránce 475.

Pokud byl kanál změněn z použití aliasu CipherSpec na použití AT-TLS, kanál připojení klienta bude používat zásadu z produktu “Konfigurace AT-TLS v odchozím kanálu pro správce front IBM MQ for Multiplatforms s použitím aliasu CipherSpecs” na stránce 470 a kanál připojení serveru bude používat zásadu z produktu “Konfigurace AT-TLS v příchozím kanálu ze správce front IBM MQ for Multiplatforms pomocí aliasu CipherSpec” na stránce 479.

Scénář 3

Mezi správcem front IBM MQ for z/OS a správcem front spuštěným v systému IBM MQ for Multiplatforms, kde správce front IBM MQ for z/OS používá protokol AT-TLS a správce front IBM MQ for Multiplatforms používá protokol IBM MQ TLS, zadáním atributu SSLCIPH s jedním názvem CipherSpec. To platí pro všechny typy kanálů zpráv jiné než odesílatele klastru a příjemce klastru.

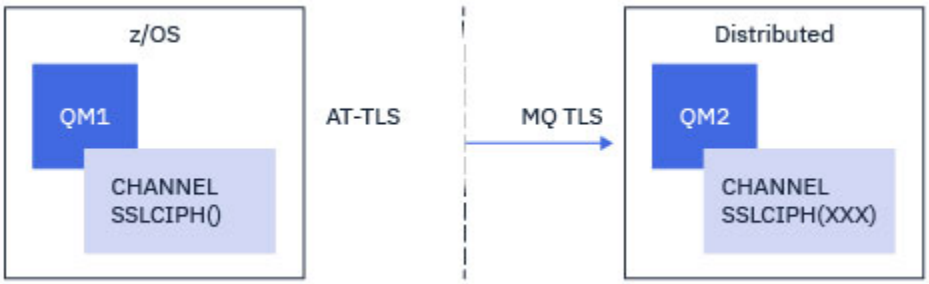


Příklad konfigurace AT-TLS pro odchozí kanály ze správce front IBM MQ for z/OS do správce front IBM MQ for Multiplatforms naleznete v tématu “Konfigurace AT-TLS v odchozím kanálu pro správce front IBM MQ for Multiplatforms s použitím jednoho názvu s názvem CipherSpec” na stránce 466 a příklad konfigurace AT-TLS pro příchozí kanály ze správce front IBM MQ for Multiplatforms do správce front IBM MQ for z/OS naleznete v tématu “Konfigurace AT-TLS v příchozím kanálu ze správce front IBM MQ for Multiplatforms s použitím jediného názvu CipherSpec” na stránce 475 .

Stejnou konfiguraci AT-TLS lze použít v případě, že jsou oba správci front v systému z/OS, ale správce front na pravé straně nebyl nakonfigurován pro použití AT-TLS.

Scénář 4

Mezi správcem front IBM MQ for z/OS a správcem front spuštěným v systému IBM MQ for Multiplatforms, kde správce front IBM MQ for z/OS používá protokol AT-TLS a správce front IBM MQ for Multiplatforms používá protokol IBM MQ TLS, zadáním atributu SSLCIPH s aliasem CipherSpec. To platí pro všechny typy kanálů zpráv jiné než odesílatele klastru a příjemce klastru.

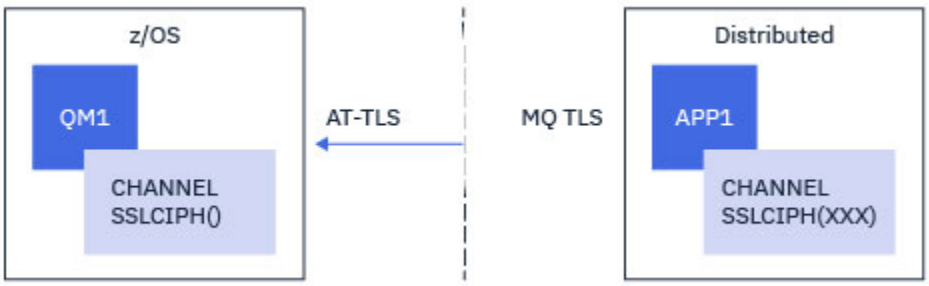


Viz “Konfigurace AT-TLS v odchozím kanálu pro správce front IBM MQ for Multiplatforms s použitím aliasu CipherSpecs” na stránce 470 , kde je uveden příklad konfigurace AT-TLS pro odchozí kanály ze správce front IBM MQ for z/OS do správce front IBM MQ for Multiplatforms a “Konfigurace AT-TLS v příchozím kanálu ze správce front IBM MQ for Multiplatforms pomocí aliasu CipherSpec” na stránce 479, a “Konfigurace AT-TLS v příchozím kanálu ze správce front IBM MQ for Multiplatforms pomocí aliasu CipherSpec” na stránce 479 , kde je uveden příklad konfigurace AT-TLS pro příchozí kanály ze správce front IBM MQ for Multiplatforms do správce front IBM MQ for z/OS .

Stejnou konfiguraci AT-TLS lze použít v případě, že jsou oba správci front v systému z/OS, ale správce front na pravé straně nebyl nakonfigurován pro použití AT-TLS.

Scénář 5

Mezi správcem front IBM MQ for z/OS a klientskou aplikací spuštěnou v systému IBM MQ for Multiplatforms, kde správce front IBM MQ for z/OS používá protokol AT-TLS a klientská aplikace používá protokol IBM MQ TLS, zadáním atributu SSLCIPH s jedním názvem CipherSpec.

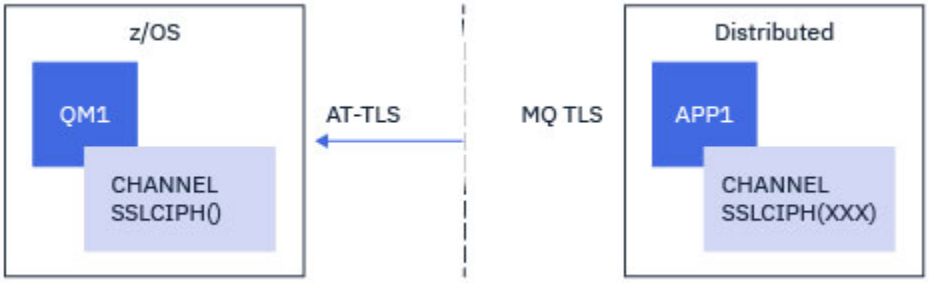


Tento scénář vyžaduje jedinou zásadu AT-TLS, která splňuje stejné požadavky jako ty, které používá kanál příchozích zpráv; viz “Konfigurace AT-TLS v příchozím kanálu ze správce front IBM MQ for Multiplatforms s použitím jediného názvu CipherSpec” na stránce 475.

Stejnou konfiguraci AT-TLS lze použít, když je klientská aplikace aplikací Java a je také spuštěna na systému z/OS, ale nebyla nakonfigurována pro použití AT-TLS.

Scénář 6

Mezi správcem front IBM MQ for z/OS a klientskou aplikací spuštěnou v systému IBM MQ for Multiplatforms, kde správce front IBM MQ for z/OS používá protokol AT-TLS a klientská aplikace používá protokol IBM MQ TLS, zadáním atributu SSLCIPH s aliasem CipherSpec.



Tento scénář vyžaduje jedinou zásadu AT-TLS, která splňuje stejné požadavky jako ty, které používá kanál příchozích zpráv; viz “Konfigurace AT-TLS v příchozím kanálu ze správce front IBM MQ for Multiplatforms pomocí aliasu CipherSpec” na stránce 479.

Stejnou konfiguraci AT-TLS lze použít, když je klientská aplikace aplikací Java a je také spuštěna na systému z/OS, ale nebyla nakonfigurována pro použití AT-TLS.

Omezení

Produkt IBM MQ for z/OS si neuvědomuje protokol AT-TLS, proto existuje několik omezení, která se vztahují na předchozí scénáře:

- AT-TLS v kombinaci s protokolem IBM MQ TLS nepracuje s kanály odesilatele klastru a příjemce klastru.
- Správci front systému IBM MQ for z/OS si nejsou vědomi toho, že používají protokol AT-TLS a nepřijímají od svého partnerského správce front nebo klienta žádné informace o certifikátu. Proto následující atributy nemají žádný vliv na z/OS stranu kanálu používajícího AT-TLS:
  - Atributy kanálu SSLCAUTH a SSLPEER
  - Atribut správce front SSLRKEYC
  - Atributy SSLPEERMAP pravidel CHLAUTH
- Použití opětovného vyjednávání tajného klíče TLS vyžaduje, aby obě strany kanálu používaly protokol IBM MQ TLS. Správce front IBM MQ for Multiplatforms nebo klient by proto neměl mít povoleno opětné vyjednávání tajného klíče TLS, pokud se připojujete ke správci front IBM MQ for z/OS pomocí AT-TLS.

Chcete-li zakázat opětné vyjednávání tajného klíče TLS pro správce front, nastavte parametr SSLRKEYC správce front na hodnotu 0. Pro klienta nastavte příslušný parametr na hodnotu 0 v závislosti na typu klienta. Podrobnosti o tom, jak to provést, viz “Resetování tajných klíčů SSL a TLS” na stránce 483.

Konfigurační příkazy AT-TLS

AT-TLS se konfiguruje pomocí sady příkazů. Ve scénářích dokumentovaných v tomto tématu se používají následující:

TTLSRule
Určuje sadu kritérií pro přiřazení připojení TCP/IP ke konfiguraci TLS. To zase odkazuje na ostatní typy příkazů.

TTLSGroupAction
Určuje, zda je odkazování `TTLSRule` povoleno či nikoli.

TTLSEnvironmentAction
Určuje podrobnou konfiguraci pro odkazující `TTLSRule` a odkazuje na řadu dalších příkazů.

TTLSKeyringParms
Odkazuje na svazek klíčů, který má používat AT-TLS.

TTLSCipherParms
Definuje šifrovací sady, které se mají použít.

TTLSEnvironmentAdvancedParms
Definuje, které protokoly TLS nebo SSL jsou povoleny.

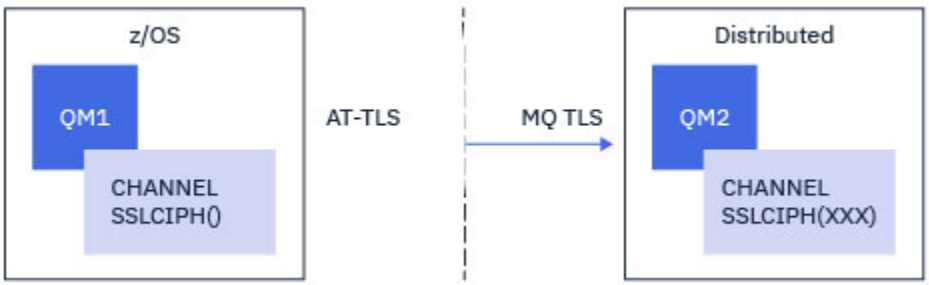
Upozornění: Existují další příkazy zásad AT-TLS s AT-TLS, které zde nejsou dokumentovány, a v závislosti na potřebě je lze použít s produktem IBM MQ . Produkt IBM MQ však byl testován pouze se zásadami popsanými v tomto tématu.

Konfigurace AT-TLS v odchozím kanálu pro správce front IBM MQ for Multiplatforms s použitím jednoho názvu s názvem CipherSpec

Způsob nastavení protokolu AT-TLS v odchozím kanálu ze správce front IBM MQ for z/OS do správce front IBM MQ for Multiplatforms . V tomto případě je kanál ve správci front z/OS odesílacím kanálem, který nemá nastaven atribut SSLCIPH, a kanál v jiném správci front nežz/OS je přijímacím kanálem s atributem SSLCIPH nastaveným na jediný kanál s názvem CipherSpec.

Příklad použití aliasu CipherSpecnaleznete v části “Konfigurace AT-TLS v odchozím kanálu pro správce front IBM MQ for Multiplatforms s použitím aliasu CipherSpecs” na stránce 470 .

V tomto příkladu se existující dvojice kanálů odesilatele a příjemce, která používá protokol TLS 1.3 TLS_AES_256_GCM_SHA384 CipherSpec , upraví tak, aby kanál odesilatele používal protokol AT-TLS namísto protokolu IBM MQ TLS.



Další protokoly TLS a CipherSpecs lze použít při menších úpravách konfigurace. Jiné typy kanálů zpráv, kromě odesílacích kanálů klastru a přijímacích kanálů klastru, lze použít beze změny v konfiguraci AT-TLS.

Postup

Krok 1: Zastavit kanál

Krok 2: Vytvoření a použití zásady AT-TLS

Pro tento scénář je třeba vytvořit následující příkazy AT-TLS:

1. Příkaz TTLSRule pro porovnání odchozích připojení z adresního prostoru inicializátoru kanálu s adresou IP a číslem portu cílového přijímacího kanálu. Tyto hodnoty by měly odpovídat informacím použitému v CONNAME kanálu odesilatele. Zde bylo zahrnuto další filtrování, aby se shodovalo s určitým názvem úlohy inicializátoru kanálu.

```
TTLSRule                        CSQ1-TO-REMOTE
{
  LocalAddr                     ALL
  RemoteAddr                    123.456.78.9
  RemotePortRange               1414
  Jobname                       CSQ1CHIN
  Direction                     OUTBOUND
  TTLSGroupActionRef            CSQ1-GROUP-ACTION
  TTLSEnvironmentActionRef      CSQ1-OUTBOUND-ENVIRONMENT-ACTION
}
```

   Předchozí pravidlo se shoduje s připojeními k adrese IP 123.456.78.9 na portu 1414 z úlohy CSQ1CHIN .

   Rozšířené volby filtrování jsou popsány v tématu TTLSRule.

2. Příkaz TTLSGroupAction povolující pravidlo. TTLSRule odkazuje na TTLSGroupAction pomocí vlastnosti **TTLSGroupActionRef** .

```
TTLSGroupAction             CSQ1-GROUP-ACTION
{
  TTLSEnabled               ON
}
```

3. Příkaz TTLSEnvironmentAction přidružený k TTLSRule vlastností **TTLSEnvironmentActionRef** . Produkt TTLSEnvironmentAction konfiguruje prostředí TLS a určuje, který svazek klíčů se má použít.

```
TTLSEnvironmentAction               CSQ1-OUTBOUND-ENVIRONMENT-ACTION
{
  HandshakeRole                     CLIENT
  TTLSKeyringParmsRef               CSQ1-KEYRING
  TTLSCipherParmsRef                CSQ1-CIPHERPARM
  TTLSEnvironmentAdvancedParmsRef   CSQ1-ENVIRONMENT-ADVANCED
}
```

4. Příkaz TTLSKeyringParms přidružený k objektu TTLSEnvironmentAction vlastností **TTLSKeyringParmsRef** a definuje svazek klíčů používaný protokolem AT-TLS.

   Svazek klíčů by měl obsahovat certifikáty důvěryhodné pro vzdáleného správce front, který neníz/OS . Tento svazek klíčů lze definovat stejným způsobem jako svazek klíčů používaný inicializátorem kanálu; viz “Konfigurace systému z/OS pro použití TLS” na stránce 256.

```
TTLSKeyringParms            CSQ1-KEYRING
{
  Keyring                   MQCHIN/CSQ1RING
}
```

5. Příkaz TTLSCipherParms přidružený k vlastnosti TTLSEnvironmentAction pomocí vlastnosti **TTLSCipherParmsRef** .

   Tento příkaz musí obsahovat jeden název šifrovací sady, který musí být ekvivalentem názvu IBM MQ CipherSpec použitého v cílovém přijímacím kanálu.

Poznámka: Názvy šifrovacích sad AT-TLS nemusí nutně odpovídat názvům IBM MQ CipherSpec . Je však možné najít název šifrovací sady AT-TLS, který odpovídá názvu IBM MQ CipherSpec , vyhledáním názvu IBM MQ CipherSpec v následující tabulce a křížovým odkazem na sloupec hexadecimálního kódu se sloupcem rozbaleného znaku z tabulky 2 v tématu příkazu TTLSCipherParms .

Tabulka 83. CipherSpecs na z/OS z IBM MQ for z/OS 9.2.0

CipherSpec	Protokol	Hexadecimální kód	Standardně povoleno
TLS_CHACHA20_POLY1305_SHA256	TLS 1.3	1303	Ano
TLS_AES_256_GCM_SHA384	TLS 1.3	1302	Ano
TLS_AES_128_GCM_SHA256	TLS 1.3	1301	Ano
TLS_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2	009D	Ano
ECDHE_RSA_AES_256_GCM_SHA384	TLS 1.2	C030	Ano
TLS_RSA_WITH_AES_256_CBC_SHA256	TLS 1.2	003D	Ano
ECDHE_ECDSA_AES_256_CBC_SHA384	TLS 1.2	C024	Ano
ECDHE_RSA_AES_256_CBC_SHA384	TLS 1.2	C028	Ano
TLS_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2	009C	Ano
ECDHE_RSA_AES_128_GCM_SHA256	TLS 1.2	C02F	Ano
TLS_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2	003C	Ano
ECDHE_ECDSA_AES_128_CBC_SHA256	TLS 1.2	C023	Ano
ECDHE_RSA_AES_128_CBC_SHA256	TLS 1.2	C027	Ano
TLS_RSA_WITH_NULL_SHA256	TLS 1.2	003B	Ne
TLS_RSA_WITH_AES_256_CBC_SHA	TLS 1.0	0035	Ne
TLS_RSA_WITH_AES_128_CBC_SHA	TLS 1.0	002F	Ne
TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS 1.0	000A	Ne
TLS_RSA_WITH_RC4_128_SHA	TLS 1.0	0005	Ne
TLS_RSA_WITH_DES_CBC_SHA	TLS 1.0	0005	Ne

Tabulka 83. CipherSpecs na z/OS z IBM MQ for z/OS 9.2.0 (pokračování)			
CipherSpec	**Protokol**	**Hexadecimální kód**	**Standardně povoleno**
TRIPLE_DES_SHA_US	SSL v3	000A	Ne
RC4_SHA_US	SSL v3	0005	Ne
RC4_MD5_US	SSL v3	0004	Ne
DES_SHA_EXPORT	SSL v3	0005	N
RC4_MD5_EXPORT	SSL v3	0003	Ne
RC2_MD5_EXPORT	SSL v3	0006	Ne
NULL_SHA	SSL v3	0002	Ne
NULL_MD5	SSL v3	0001	Ne

```
TTLSCipherParms             CSQ1-CIPHERPARM
{
  V3CipherSuites            TLS_AES_256_GCM_SHA384
}
```

6. Příkaz TTLSEnvironmentAdvancedParms je přidružen k `TTLSEnvironmentAction` pomocí vlastnosti **`TTLSEnvironmentAdvancedParmsRef`** .

   Tento příkaz lze použít k určení, které protokoly SSL a TLS jsou povoleny. S produktem IBM MQ byste měli povolit pouze jediný protokol, který odpovídá názvu šifrovací sady použitému v příkazu `TTLSCipherParms` .

```
TTLSEnvironmentAdvancedParms CSQ1-ENVIRONMENT-ADVANCED
{
  SSLv3           OFF
  TLSv1           OFF
  TLSv1.1         OFF
  SecondaryMap    OFF
  TLSv1.2         OFF
  TLSv1.3         ON
}
```

Úplná sada příkazů je následující a měla by být použita na agenta zásad:

```
TTLSRule                      CSQ1-TO-REMOTE
{
  LocalAddr                   ALL
  RemoteAddr                  123.456.78.9
  RemotePortRange             1414
  Jobname                     CSQ1CHIN
  Direction                   OUTBOUND
  TTLSGroupActionRef          CSQ1-GROUP-ACTION
  TTLSEnvironmentActionRef    CSQ1-OUTBOUND-ENVIRONMENT-ACTION
}

TTLSGroupAction             CSQ1-GROUP-ACTION
{
  TTLSEnabled               ON
}

TTLSEnvironmentAction             CSQ1-OUTBOUND-ENVIRONMENT-ACTION
{
  HandshakeRole                   CLIENT
  TTLSKeyringParmsRef             CSQ1-KEYRING
  TTLSCipherParmsRef              CSQ1-CIPHERPARM
  TTLSEnvironmentAdvancedParmsRef CSQ1-ENVIRONMENT-ADVANCED
}

TTLSKeyringParms            CSQ1-KEYRING
{
  Keyring                   MQCHIN/CSQ1RING
}

TTLSCipherParms             CSQ1-CIPHERPARM
{
  V3CipherSuites            TLS_AES_256_GCM_SHA384
}

TTLSEnvironmentAdvancedParms CSQ1-ENVIRONMENT-ADVANCED
{
  SSLv3          OFF
  TLSv1          OFF
  TLSv1.1        OFF
  SecondaryMap   OFF
  TLSv1.2        OFF
  TLSv1.3        ON
}
```

Krok 3: Odebrat SSLCIPH z z/OS kanálu

Odeberte specifikaci CipherSpec z kanálu z/OS pomocí následujícího příkazu:

```
ALTER CHANNEL(channel-name) CHLTYPE(SDR) SSLCIPH(' ')
```

Krok 4: Spuštění kanálu

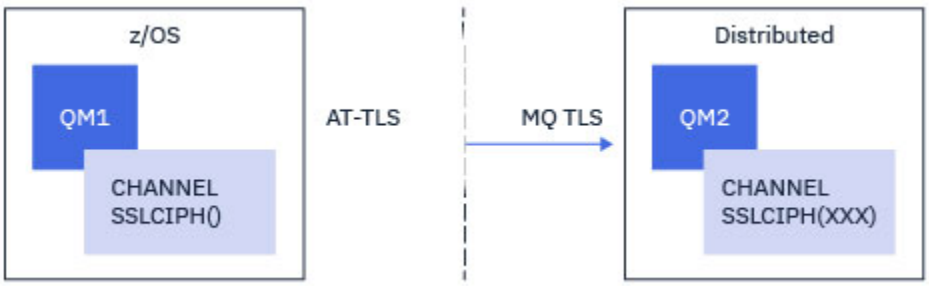
Jakmile je kanál spuštěn, bude používat kombinaci AT-TLS a IBM MQ TLS.

Upozornění: Předchozí příkazy AT-TLS jsou pouze minimální konfigurací. Existují další příkazy zásad AT-TLS s AT-TLS, které zde nejsou dokumentovány, a v závislosti na potřebě je lze použít s produktem IBM MQ . Produkt IBM MQ však byl testován pouze s popsanými zásadami.

Konfigurace AT-TLS v odchozím kanálu pro správce front IBM MQ for Multiplatforms s použitím aliasu CipherSpecs

Způsob nastavení protokolu AT-TLS v odchozím kanálu ze správce front IBM MQ for z/OS do správce front IBM MQ for Multiplatforms . V tomto případě je kanál ve správci front z/OS odesílacím kanálem, který nemá nastaven atribut SSLCIPH, a kanál v jiném správci front nežz/OS je přijímacím kanálem s atributem SSLCIPH nastaveným na alias CipherSpec .

V tomto příkladu bude upravena existující dvojice kanálu odesilatele a příjemce, která používá alias ANY_TLS13 CipherSpec , aby kanál odesilatele používal protokol AT-TLS namísto protokolu IBM MQ TLS.



Jiné protokoly TLS a CiperSpecs lze použít provedením menších úprav v konfiguraci. Jiné typy kanálů zpráv, kromě odesílacích kanálů klastru a přijímacích kanálů klastru, lze použít beze změny v konfiguraci AT-TLS.

Postup

Krok 1: Zastavit kanál

Krok 2: Vytvoření a použití zásady AT-TLS

Pro tento scénář je třeba vytvořit následující příkazy AT-TLS:

1. Příkaz TTLSRule pro porovnání odchozích připojení z adresního prostoru inicializátoru kanálu s adresou IP a číslem portu cílového přijímacího kanálu. Tyto hodnoty by měly odpovídat informacím použitému v CONNAME kanálu odesilatele. Zde bylo zahrnuto další filtrování, aby se shodovalo s určitým názvem úlohy inicializátoru kanálu.

```
TTLSRule                        CSQ1-TO-REMOTE
{
  LocalAddr                     ALL
  RemoteAddr                    123.456.78.9
  RemotePortRange               1414
  Jobname                       CSQ1CHIN
  Direction                     OUTBOUND
  TTLSGroupActionRef            CSQ1-GROUP-ACTION
  TTLSEnvironmentActionRef      CSQ1-OUTBOUND-ENVIRONMENT-ACTION
}
```

   Předchozí pravidlo se shoduje s připojeními k adrese IP 123.456.78.9 na portu 1414 z úlohy CSQ1CHIN .

   Rozšířené volby filtrování jsou popsány v tématu TTLSRule.

2. Příkaz TTLSGroupAction povolující pravidlo. TTLSRule odkazuje na TTLSGroupAction pomocí vlastnosti **TTLSGroupActionRef** .

```
TTLSGroupAction             CSQ1-GROUP-ACTION
{
  TTLSEnabled               ON
}
```

3. Příkaz TTLSEnvironmentAction přidružený k TTLSRule vlastností **TTLSEnvironmentActionRef** . Produkt TTLSEnvironmentAction konfiguruje prostředí TLS a určuje, který svazek klíčů se má použít.

```
TTLSEnvironmentAction               CSQ1-OUTBOUND-ENVIRONMENT-ACTION
{
  HandshakeRole                     CLIENT
  TTLSKeyringParmsRef               CSQ1-KEYRING
  TTLSCipherParmsRef                CSQ1-CIPHERPARM
  TTLSEnvironmentAdvancedParmsRef   CSQ1-ENVIRONMENT-ADVANCED
}
```

4. Příkaz TTLSKeyringParms přidružený k objektu TTLSEnvironmentAction vlastností **TTLSKeyringParmsRef** a definuje svazek klíčů používaný protokolem AT-TLS.

   Svazek klíčů by měl obsahovat certifikáty důvěryhodné pro vzdáleného správce front, který neníz/OS . Tento svazek klíčů lze definovat stejným způsobem jako svazek klíčů používaný inicializátorem kanálu; viz “Konfigurace systému z/OS pro použití TLS” na stránce 256.

```
TTLSKeyringParms            CSQ1-KEYRING
{
  Keyring                   MQCHIN/CSQ1RING
}
```

5. Příkaz TTLSCipherParms přidružený k vlastnosti TTLSEnvironmentAction pomocí vlastnosti **TTLSCipherParmsRef** .

   Tento příkaz musí obsahovat jeden nebo více názvů šifrovacích sad, z nichž alespoň jeden by měl být kompatibilní se sadou specifikací CipherSpecs odvozenou z aliasu CipherSpec použitého v cílovém přijímacím kanálu.

   Poznámka: Názvy šifrovacích sad AT-TLS nemusí nutně odpovídat názvům IBM MQ CipherSpec . Je však možné vyhledat název šifrovací sady AT-TLS, který odpovídá názvu IBM MQ CipherSpec , vyhledáním názvu IBM MQ CipherSpec v následující tabulce a křížovým odkazem na sloupec hexadecimálního kódu se sloupcem rozbaleného znaku z tabulky 2 v tématu TTLSCipherParms .

Tabulka 84. CipherSpecs na z/OS z IBM MQ for z/OS 9.2.0

CipherSpec	Protokol	Hexadecimální kód	Standardně povoleno
TLS_CHACHA20_POLY1305_SHA256	TLS 1.3	1303	Ano
TLS_AES_256_GCM_SHA384	TLS 1.3	1302	Ano
TLS_AES_128_GCM_SHA256	TLS 1.3	1301	Ano
TLS_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2	009D	Ano
ECDHE_RSA_AES_256_GCM_SHA384	TLS 1.2	C030	Ano
TLS_RSA_WITH_AES_256_CBC_SHA256	TLS 1.2	003D	Ano
ECDHE_ECDSA_AES_256_CBC_SHA384	TLS 1.2	C024	Ano
ECDHE_RSA_AES_256_CBC_SHA384	TLS 1.2	C028	Ano
TLS_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2	009C	Ano
ECDHE_RSA_AES_128_GCM_SHA256	TLS 1.2	C02F	Ano

Tabulka 84. CipherSpecs na z/OS z IBM MQ for z/OS 9.2.0 (pokračování)			
CipherSpec	**Protokol**	**Hexadecimální kód**	**Standardně povoleno**
TLS_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2	003C	Ano
ECDHE_ECDSA_AES_128_CBC_SHA256	TLS 1.2	C023	Ano
ECDHE_RSA_AES_128_CBC_SHA256	TLS 1.2	C027	Ano
TLS_RSA_WITH_NULL_SHA256	TLS 1.2	003B	Ne
TLS_RSA_WITH_AES_256_CBC_SHA	TLS 1.0	0035	Ne
TLS_RSA_WITH_AES_128_CBC_SHA	TLS 1.0	002F	Ne
TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS 1.0	000A	Ne
TLS_RSA_WITH_RC4_128_SHA	TLS 1.0	0005	Ne
TLS_RSA_WITH_DES_CBC_SHA	TLS 1.0	0005	Ne
TRIPLE_DES_SHA_US	SSL v3	000A	Ne
RC4_SHA_US	SSL v3	0005	Ne
RC4_MD5_US	SSL v3	0004	Ne
DES_SHA_EXPORT	SSL v3	0005	N
RC4_MD5_EXPORT	SSL v3	0003	Ne
RC2_MD5_EXPORT	SSL v3	0006	Ne
NULL_SHA	SSL v3	0002	Ne
NULL_MD5	SSL v3	0001	Ne

```
TTLSCipherParms             CSQ1-CIPHERPARM
{
  V3CipherSuites            TLS_CHACHA20_POLY1305_SHA256
  V3CipherSuites            TLS_AES_256_GCM_SHA384
  V3CipherSuites            TLS_AES_128_GCM_SHA256
}
```

Upozornění: Pokud správce front i zásada AT-TLS podporují protokol TLS 1.3, umožní spuštění kanálu pouze alias CipherSpecs obsahující alespoň jeden protokol TLS 1.3 CipherSpec . Například použití ANY_TLS12 má za následek neúspěšné spuštění kanálu, a to i v případě, že TTLSCipherParms obsahuje protokol TLS 1.2 CipherSpecs, ale použití ANY_TLS12_OR_HIGHER nebo ANY_TLS13 umožňuje spuštění kanálu. Vysvětlení viz “Relace mezi nastaveními aliasu CipherSpec” na stránce 458 .

6. Příkaz TTLSEnvironmentAdvancedParms je přidružen k `TTLSEnvironmentAction` pomocí vlastnosti **`TTLSEnvironmentAdvancedParmsRef`** .

   Tento příkaz lze použít k určení, které protokoly SSL a TLS jsou povoleny, a měly by být konzistentní s šifrovanými sadami v příkazu `TTLSCipherParms` .

```
TTLSEnvironmentAdvancedParms CSQ1-ENVIRONMENT-ADVANCED
{
  SSLv3          OFF
  TLSv1          OFF
  TLSv1.1        OFF
  SecondaryMap   OFF
  TLSv1.2        OFF
  TLSv1.3        ON
}
```

Úplná sada příkazů je následující a měla by být použita na agenta zásad:

```
TTLSRule                      CSQ1-TO-REMOTE
{
  LocalAddr                   ALL
  RemoteAddr                  123.456.78.9
  RemotePortRange             1414
  Jobname                     CSQ1CHIN
  Direction                   OUTBOUND
  TTLSGroupActionRef          CSQ1-GROUP-ACTION
  TTLSEnvironmentActionRef    CSQ1-OUTBOUND-ENVIRONMENT-ACTION
}

TTLSGroupAction             CSQ1-GROUP-ACTION
{
  TTLSEnabled               ON
}

TTLSEnvironmentAction             CSQ1-OUTBOUND-ENVIRONMENT-ACTION
{
  HandshakeRole                   CLIENT
  TTLSKeyringParmsRef             CSQ1-KEYRING
  TTLSCipherParmsRef              CSQ1-CIPHERPARM
  TTLSEnvironmentAdvancedParmsRef CSQ1-ENVIRONMENT-ADVANCED
}

TTLSKeyringParms            CSQ1-KEYRING
{
  Keyring                   MQCHIN/CSQ1RING
}

TTLSCipherParms             CSQ1-CIPHERPARM
{
  V3CipherSuites            TLS_CHACHA20_POLY1305_SHA256
  V3CipherSuites            TLS_AES_256_GCM_SHA384
  V3CipherSuites            TLS_AES_128_GCM_SHA256

}

TTLSEnvironmentAdvancedParms CSQ1-ENVIRONMENT-ADVANCED
{
  SSLv3          OFF
  TLSv1          OFF
  TLSv1.1        OFF
  SecondaryMap   OFF
  TLSv1.2        OFF
  TLSv1.3        ON
}
```

Krok 3: Odebrat SSLCIPH z z/OS kanálu

Odeberte specifikaci CipherSpec z kanálu z/OS pomocí následujícího příkazu:

```
ALTER CHANNEL(channel-name) CHLTYPE(SDR) SSLCIPH(' ')
```

Krok 4: Spuštění kanálu

Jakmile je kanál spuštěn, bude používat kombinaci AT-TLS a IBM MQ TLS.

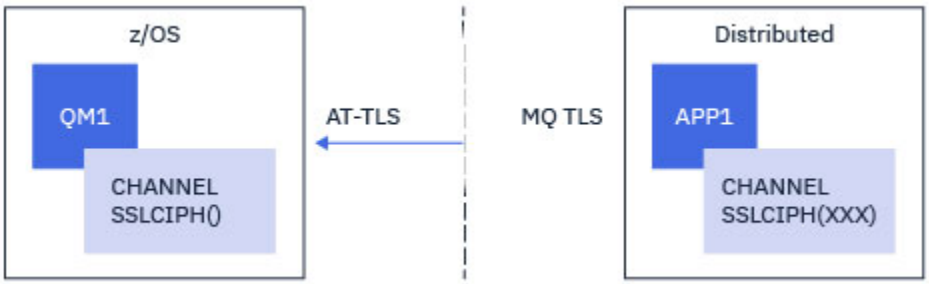
Upozornění: Předchozí příkazy AT-TLS jsou pouze minimální konfigurací. Existují další příkazy zásad AT-TLS s AT-TLS, které zde nejsou dokumentovány, a v závislosti na potřebě je lze použít s produktem IBM MQ . Produkt IBM MQ však byl testován pouze s popsanými zásadami.

Konfigurace AT-TLS v příchozím kanálu ze správce front IBM MQ for Multiplatforms s použitím jediného názvu CipherSpec

Způsob nastavení AT-TLS v příchozím kanálu ze správce front IBM MQ for Multiplatforms do správce front IBM MQ for z/OS . V tomto případě je kanál ve správci front z/OS přijímacím kanálem, který nemá nastaven atribut SSLCIPH, a kanál ve správci front jiného typu nežz/OS je odesílacím kanálem s atributem SSLCIPH nastaveným na jediný kanál s názvem CipherSpec.

Příklad použití aliasu CipherSpecnaleznete v části “Konfigurace AT-TLS v příchozím kanálu ze správce front IBM MQ for Multiplatforms pomocí aliasu CipherSpec” na stránce 479 .

V tomto příkladu se existující dvojice kanálů odesilatele a příjemce, která používá protokol TLS 1.3 TLS_AES_256_GCM_SHA384 CipherSpec , upraví tak, aby přijímací kanál používal protokol AT-TLS namísto protokolu IBM MQ TLS.



Další protokoly TLS a CipherSpecs lze použít při menších úpravách konfigurace. Jiné typy kanálů zpráv, kromě odesílacích kanálů klastru a přijímacích kanálů klastru, lze použít beze změny v konfiguraci AT-TLS.

Postup

Krok 1: Zastavit kanál

Krok 2: Vytvoření a použití zásady AT-TLS

Pro tento scénář je třeba vytvořit následující příkazy AT-TLS:

1. Příkaz TTLSRule pro porovnání příchozích připojení s adresním prostorem inicializátoru kanálu z adresy IP kanálu odesilatele. Zde bylo zahrnuto další filtrování, aby se shodovalo s určitým názvem úlohy inicializátoru kanálu.

```
TTLSRule                        REMOTE-TO-CSQ1
{
  LocalAddr                     ALL
  LocalPortRange                1414
  RemoteAddr                    123.456.78.9
  Jobname                       CSQ1CHIN
  Direction                     INBOUND
  TTLSGroupActionRef            CSQ1-GROUP-ACTION
  TTLSEnvironmentActionRef      CSQ1-INBOUND-ENVIRONMENT-ACTION
}
```

   Předchozí pravidlo se shoduje s připojeními přicházejícími do úlohy CSQ1CHIN na lokálním portu 1414 ze vzdálené adresy IP 123.456.78.9.

   Rozšířené volby filtrování jsou popsány v tématu TTLSRule.

2. Příkaz TTLSGroupAction povolující pravidlo. `TTLSRule` odkazuje na `TTLSGroupAction` pomocí vlastnosti **`TTLSGroupActionRef`** .

```
TTLSGroupAction             CSQ1-GROUP-ACTION
{
  TTLSEnabled               ON
}
```

3. Příkaz TTLSEnvironmentAction je přidružen k TTLSRule pomocí vlastnosti **TTLSEnvironmentActionRef** . Produkt TTLSEnvironmentAction konfiguruje prostředí TLS a určuje, který svazek klíčů se má použít.

```
TTLSEnvironmentAction                CSQ1-INBOUND-ENVIRONMENT-ACTION
{
  HandshakeRole                      SERVER
  TTLSKeyringParmsRef                CSQ1-KEYRING
  TTLSCipherParmsRef                 CSQ1-CIPHERPARM
  TTLSEnvironmentAdvancedParmsRef    CSQ1-ENVIRONMENT-ADVANCED
}
```

AT-TLS poskytuje schopnost poskytovat vzájemné ověření, což je ekvivalent použití atributu kanálu SSLCAUTH. To se provádí pomocí příkazu TTLSEnvironmentAction s hodnotou **HandshakeRole** *ServerWithClientAuth* pro příchozí příkaz TTLSEnvironmentAction .

4. Příkaz TTLSKeyringParms je přidružen k TTLSEnvironmentAction vlastností **TTLSKeyringParmsRef** a definuje svazek klíčů používaný AT-TLS.

   Svazek klíčů by měl obsahovat certifikáty důvěryhodné pro vzdáleného správce front, který neníz/OS . Tento svazek klíčů lze definovat stejným způsobem jako svazek klíčů používaný inicializátorem kanálu; viz “Konfigurace systému z/OS pro použití TLS” na stránce 256.

```
TTLSKeyringParms            CSQ1-KEYRING
{
  Keyring                   MQCHIN/CSQ1RING
}
```

5. Příkaz TTLSCipherParms přidružený k vlastnosti TTLSEnvironmentAction pomocí vlastnosti **TTLSCipherParmsRef** .

   Tento příkaz musí obsahovat jeden název šifrovací sady, který musí být ekvivalentem názvu IBM MQ CipherSpec použitého ve vzdáleném kanálu odesilatele.

   Poznámka: Názvy šifrovacích sad AT-TLS nemusí nutně odpovídat názvům IBM MQ CipherSpec . Je však možné najít název šifrovací sady AT-TLS, který odpovídá názvu IBM MQ CipherSpec , vyhledáním názvu IBM MQ CipherSpec v následující tabulce a křížovým odkazem na sloupec hexadecimálního kódu se sloupcem rozbaleného znaku z tabulky 2 v tématu příkazu TTLSCipherParms .

Tabulka 85. CipherSpecs na z/OS z IBM MQ for z/OS 9.2.0

CipherSpec	Protokol	Hexadecimální kód	Standardně povoleno
TLS_CHACHA20_POLY1305_SHA256	TLS 1.3	1303	Ano
TLS_AES_256_GCM_SHA384	TLS 1.3	1302	Ano
TLS_AES_128_GCM_SHA256	TLS 1.3	1301	Ano
TLS_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2	009D	Ano
ECDHE_RSA_AES_256_GCM_SHA384	TLS 1.2	C030	Ano

Tabulka 85. CipherSpecs na z/OS z IBM MQ for z/OS 9.2.0 (pokračování)			
CipherSpec	**Protokol**	**Hexadecimální kód**	**Standardně povoleno**
TLS_RSA_WITH_AES_256_CBC_SHA256	TLS 1.2	003D	Ano
ECDHE_ECDSA_AES_256_CBC_SHA384	TLS 1.2	C024	Ano
ECDHE_RSA_AES_256_CBC_SHA384	TLS 1.2	C028	Ano
TLS_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2	009C	Ano
ECDHE_RSA_AES_128_GCM_SHA256	TLS 1.2	C02F	Ano
TLS_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2	003C	Ano
ECDHE_ECDSA_AES_128_CBC_SHA256	TLS 1.2	C023	Ano
ECDHE_RSA_AES_128_CBC_SHA256	TLS 1.2	C027	Ano
TLS_RSA_WITH_NULL_SHA256	TLS 1.2	003B	Ne
TLS_RSA_WITH_AES_256_CBC_SHA	TLS 1.0	0035	Ne
TLS_RSA_WITH_AES_128_CBC_SHA	TLS 1.0	002F	Ne
TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS 1.0	000A	Ne
TLS_RSA_WITH_RC4_128_SHA	TLS 1.0	0005	Ne
TLS_RSA_WITH_DES_CBC_SHA	TLS 1.0	0005	Ne
TRIPLE_DES_SHA_US	SSL v3	000A	Ne
RC4_SHA_US	SSL v3	0005	Ne
RC4_MD5_US	SSL v3	0004	Ne
DES_SHA_EXPORT	SSL v3	0005	N
RC4_MD5_EXPORT	SSL v3	0003	Ne
RC2_MD5_EXPORT	SSL v3	0006	Ne
NULL_SHA	SSL v3	0002	Ne
NULL_MD5	SSL v3	0001	Ne

```
TTLSCipherParms             CSQ1-CIPHERPARM
{
  V3CipherSuites            TLS_AES_256_GCM_SHA384
}
```

6. Příkaz TTLSEnvironmentAdvancedParms je přidružen k TTLSEnvironmentAction pomocí vlastnosti **TTLSEnvironmentAdvancedParmsRef** .

   Tento příkaz lze použít k určení, které protokoly SSL a TLS jsou povoleny. S produktem IBM MQ byste měli povolit pouze jediný protokol, který odpovídá názvu šifrovací sady použitému v příkazu TTLSCipherParms .

```
TTLSEnvironmentAdvancedParms CSQ1-ENVIRONMENT-ADVANCED
{
  SSLv3          OFF
  TLSv1          OFF
  TLSv1.1        OFF
  SecondaryMap   OFF
  TLSv1.2        OFF
  TLSv1.3        ON
}
```

Úplná sada příkazů je následující a měla by být použita na agenta zásad:

```


TTLSRule                      REMOTE-TO-CSQ1
{
  LocalAddr                   ALL
  LocalPortRange              1414
  RemoteAddr                  123.456.78.9
  Jobname                     CSQ1CHIN
  Direction                   INBOUND
  TTLSGroupActionRef          CSQ1-GROUP-ACTION
  TTLSEnvironmentActionRef    CSQ1-INBOUND-ENVIRONMENT-ACTION
}

TTLSGroupAction             CSQ1-GROUP-ACTION
{
  TTLSEnabled               ON
}

TTLSEnvironmentAction             CSQ1-INBOUND-ENVIRONMENT-ACTION
{
  HandshakeRole                   SERVER
  TTLSKeyringParmsRef             CSQ1-KEYRING
  TTLSCipherParmsRef              CSQ1-CIPHERPARM
  TTLSEnvironmentAdvancedParmsRef CSQ1-ENVIRONMENT-ADVANCED
}

TTLSKeyringParms            CSQ1-KEYRING
{
  Keyring                   MQCHIN/CSQ1RING
}

TTLSCipherParms             CSQ1-CIPHERPARM
{
  V3CipherSuites            TLS_AES_256_GCM_SHA384
}

TTLSEnvironmentAdvancedParms CSQ1-ENVIRONMENT-ADVANCED
{
  SSLv3          OFF
  TLSv1          OFF
  TLSv1.1        OFF
  SecondaryMap   OFF
  TLSv1.2        OFF
  TLSv1.3        ON
}
```

Krok 3: Odebrat SSLCIPH z z/OS kanálu

Odeberte specifikaci CipherSpec z kanálu z/OS pomocí následujícího příkazu:

```
ALTER CHANNEL(channel-name) CHLTYPE(RCVR) SSLCIPH(' ')
```

Krok 4: Spuštění kanálu

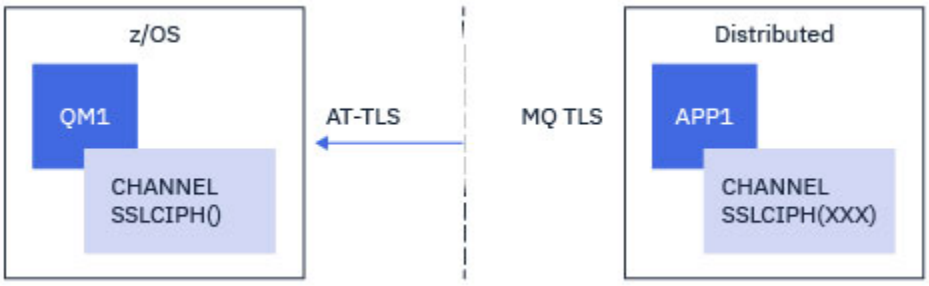
Jakmile je kanál spuštěn, bude používat kombinaci AT-TLS a IBM MQ TLS.

Upozornění: Předchozí příkazy AT-TLS jsou pouze minimální konfigurací. Existují další příkazy zásad AT-TLS s AT-TLS, které zde nejsou dokumentovány, a v závislosti na potřebě je lze použít s produktem IBM MQ . Produkt IBM MQ však byl testován pouze s popsanými zásadami.

Konfigurace AT-TLS v příchozím kanálu ze správce front IBM MQ for Multiplatforms pomocí aliasu CipherSpec

Způsob nastavení AT-TLS v příchozím kanálu ze správce front IBM MQ for Multiplatforms do správce front IBM MQ for z/OS . V tomto případě je kanál ve správci front z/OS přijímacím kanálem, který nemá nastaven atribut SSLCIPH, a kanál v jiném správci front nežz/OS je odesílacím kanálem s atributem SSLCIPH nastaveným na alias CipherSpec.

V tomto příkladu bude upravena existující dvojice odesílacích a přijímacích kanálů, která používá libovolný protokol TLS 1.3 CipherSpec , aby přijímací kanál používal protokol AT-TLS namísto protokolu IBM MQ TLS.



Jiné protokoly TLS a CiperSpecs lze použít provedením menších úprav v konfiguraci. Jiné typy kanálů zpráv, kromě odesílacích kanálů klastru a přijímacích kanálů klastru, lze použít beze změny v konfiguraci AT-TLS.

Postup

Krok 1: Zastavit kanál

Krok 2: Vytvoření a použití zásady AT-TLS

Pro tento scénář je třeba vytvořit následující příkazy AT-TLS:

1. Příkaz TTLSRule pro porovnání příchozích připojení s adresním prostorem inicializátoru kanálu z adresy IP kanálu odesilatele. Zde bylo zahrnuto další filtrování, aby se shodovalo s určitým názvem úlohy inicializátoru kanálu.

```
TTLSRule                        REMOTE-TO-CSQ1
{
  LocalAddr                     ALL
  LocalPortRange                1414
  RemoteAddr                    123.456.78.9
  Jobname                       CSQ1CHIN
  Direction                     INBOUND
  TTLSGroupActionRef            CSQ1-GROUP-ACTION
  TTLSEnvironmentActionRef      CSQ1-INBOUND-ENVIRONMENT-ACTION
}
```

   Předchozí pravidlo se shoduje s připojeními přicházejícími do úlohy CSQ1CHIN na lokálním portu 1414 ze vzdálené adresy IP 123.456.78.9.

   Rozšířené volby filtrování jsou popsány v tématu TTLSRule.

2. Příkaz TTLSGroupAction povolující pravidlo. `TTLSRule` odkazuje na `TTLSGroupAction` pomocí vlastnosti **`TTLSGroupActionRef`** .

```
TTLSGroupAction             CSQ1-GROUP-ACTION
{
  TTLSEnabled               ON
}
```

3. Příkaz TTLSEnvironmentAction je přidružen k TTLSRule pomocí vlastnosti **TTLSEnvironmentActionRef** . Produkt TTLSEnvironmentAction konfiguruje prostředí TLS a určuje, který svazek klíčů se má použít.

```
TTLSEnvironmentAction                 CSQ1-INBOUND-ENVIRONMENT-ACTION
{
  HandshakeRole                       SERVER
  TTLSKeyringParmsRef                 CSQ1-KEYRING
  TTLSCipherParmsRef                  CSQ1-CIPHERPARM
  TTLSEnvironmentAdvancedParmsRef     CSQ1-ENVIRONMENT-ADVANCED
}
```

AT-TLS poskytuje schopnost poskytovat vzájemné ověření, což je ekvivalent použití atributu kanálu SSLCAUTH. To se provádí pomocí příkazu TTLSEnvironmentAction s hodnotou **HandshakeRole** *ServerWithClientAuth* pro příchozí příkaz TTLSEnvironmentAction .

4. Příkaz TTLSKeyringParms je přidružen k TTLSEnvironmentAction vlastností **TTLSKeyringParmsRef** a definuje svazek klíčů používaný AT-TLS.

   Svazek klíčů by měl obsahovat certifikáty důvěryhodné pro vzdáleného správce front, který neníz/OS . Tento svazek klíčů lze definovat stejným způsobem jako svazek klíčů používaný inicializátorem kanálu; viz “Konfigurace systému z/OS pro použití TLS” na stránce 256.

```
TTLSKeyringParms            CSQ1-KEYRING
{
  Keyring                   MQCHIN/CSQ1RING
}
```

5. Příkaz TTLSCipherParms přidružený k vlastnosti TTLSEnvironmentAction pomocí vlastnosti **TTLSCipherParmsRef** .

   Tento příkaz musí obsahovat alespoň jeden název šifrovací sady, který je obsažen v aliasu CipherSpec nastaveném ve vzdáleném kanálu odesilatele.

   Poznámka: Názvy šifrovacích sad AT-TLS nemusí nutně odpovídat názvům IBM MQ CipherSpec . Je však možné najít název šifrovací sady AT-TLS, který odpovídá názvu IBM MQ CipherSpec , vyhledáním názvu IBM MQ CipherSpec v následující tabulce a křížovým odkazem na sloupec hexadecimálního kódu se sloupcem rozbaleného znaku z tabulky 2 v tématu příkazu TTLSCipherParms .

Tabulka 86. CipherSpecs na z/OS z IBM MQ for z/OS 9.2.0

CipherSpec	Protokol	Hexadecimální kód	Standardně povoleno
TLS_CHACHA20_POLY1305_SHA256	TLS 1.3	1303	Ano
TLS_AES_256_GCM_SHA384	TLS 1.3	1302	Ano
TLS_AES_128_GCM_SHA256	TLS 1.3	1301	Ano
TLS_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2	009D	Ano
ECDHE_RSA_AES_256_GCM_SHA384	TLS 1.2	C030	Ano

Tabulka 86. CipherSpecs na z/OS z IBM MQ for z/OS 9.2.0 (pokračování)

CipherSpec	Protokol	Hexadecimální kód	Standardně povoleno
TLS_RSA_WITH_AES_256_CBC_SHA256	TLS 1.2	003D	Ano
ECDHE_ECDSA_AES_256_CBC_SHA384	TLS 1.2	C024	Ano
ECDHE_RSA_AES_256_CBC_SHA384	TLS 1.2	C028	Ano
TLS_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2	009C	Ano
ECDHE_RSA_AES_128_GCM_SHA256	TLS 1.2	C02F	Ano
TLS_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2	003C	Ano
ECDHE_ECDSA_AES_128_CBC_SHA256	TLS 1.2	C023	Ano
ECDHE_RSA_AES_128_CBC_SHA256	TLS 1.2	C027	Ano
TLS_RSA_WITH_NULL_SHA256	TLS 1.2	003B	Ne
TLS_RSA_WITH_AES_256_CBC_SHA	TLS 1.0	0035	Ne
TLS_RSA_WITH_AES_128_CBC_SHA	TLS 1.0	002F	Ne
TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS 1.0	000A	Ne
TLS_RSA_WITH_RC4_128_SHA	TLS 1.0	0005	Ne
TLS_RSA_WITH_DES_CBC_SHA	TLS 1.0	0005	Ne
TRIPLE_DES_SHA_US	SSL v3	000A	Ne
RC4_SHA_US	SSL v3	0005	Ne
RC4_MD5_US	SSL v3	0004	Ne
DES_SHA_EXPORT	SSL v3	0005	N
RC4_MD5_EXPORT	SSL v3	0003	Ne
RC2_MD5_EXPORT	SSL v3	0006	Ne
NULL_SHA	SSL v3	0002	Ne
NULL_MD5	SSL v3	0001	Ne

```
TTLSCipherParms             CSQ1-CIPHERPARM
{
  V3CipherSuites            TLS_CHACHA20_POLY1305_SHA256
  V3CipherSuites            TLS_AES_256_GCM_SHA384
  V3CipherSuites            TLS_AES_128_GCM_SHA256
}
```

Upozornění: Pokud správce front i zásada AT-TLS podporují protokol TLS 1.3, umožní spuštění kanálu pouze alias CipherSpecs obsahující alespoň jeden protokol TLS 1.3 CipherSpec . Například použití ANY_TLS12 má za následek neúspěšné spuštění kanálu, a to i v případě, že TTLSCipherParms obsahuje protokol TLS 1.2 CipherSpecs, ale použití ANY_TLS12_OR_HIGHER nebo ANY_TLS13 umožňuje spuštění kanálu. Vysvětlení viz “Relace mezi nastaveními aliasu CipherSpec” na stránce 458 .

6. Příkaz TTLSEnvironmentAdvancedParms je přidružen k TTLSEnvironmentAction pomocí vlastnosti **TTLSEnvironmentAdvancedParmsRef** .

   Tento příkaz lze použít k určení, které protokoly SSL a TLS jsou povoleny, a měly by být konzistentní s šifrovanými sadami v příkazu TTLSCipherParms .

```
TTLSEnvironmentAdvancedParms CSQ1-ENVIRONMENT-ADVANCED
{
  SSLv3           OFF
  TLSv1           OFF
  TLSv1.1         OFF
  SecondaryMap    OFF
  TLSv1.2         OFF
  TLSv1.3         ON
}
```

Úplná sada příkazů je následující a měla by být použita na agenta zásad:

```
TTLSRule                      REMOTE-TO-CSQ1
{
  LocalAddr                   ALL
  LocalPortRange              1414
  RemoteAddr                  123.456.78.9
  Jobname                     CSQ1CHIN
  Direction                   INBOUND
  TTLSGroupActionRef          CSQ1-GROUP-ACTION
  TTLSEnvironmentActionRef    CSQ1-INBOUND-ENVIRONMENT-ACTION
}

TTLSGroupAction             CSQ1-GROUP-ACTION
{
  TTLSEnabled               ON
}

TTLSEnvironmentAction             CSQ1-INBOUND-ENVIRONMENT-ACTION
{
  HandshakeRole                   SERVER
  TTLSKeyringParmsRef             CSQ1-KEYRING
  TTLSCipherParmsRef              CSQ1-CIPHERPARM
  TTLSEnvironmentAdvancedParmsRef CSQ1-ENVIRONMENT-ADVANCED
}

TTLSKeyringParms            CSQ1-KEYRING
{
  Keyring                   MQCHIN/CSQ1RING
}

TTLSCipherParms             CSQ1-CIPHERPARM
{
  V3CipherSuites            TLS_CHACHA20_POLY1305_SHA256
  V3CipherSuites            TLS_AES_256_GCM_SHA384
  V3CipherSuites            TLS_AES_128_GCM_SHA256

}

TTLSEnvironmentAdvancedParms CSQ1-ENVIRONMENT-ADVANCED
{
  SSLv3          OFF
  TLSv1          OFF
  TLSv1.1        OFF
  SecondaryMap   OFF
  TLSv1.2        OFF
  TLSv1.3        ON
}
```

Krok 3: Odebrat SSLCIPH z z/OS kanálu

Odeberte specifikaci CipherSpec z kanálu z/OS pomocí následujícího příkazu:

```
ALTER CHANNEL(channel-name) CHLTYPE(SDR) SSLCIPH(' ')
```

Krok 4: Spuštění kanálu

Jakmile je kanál spuštěn, bude používat kombinaci AT-TLS a IBM MQ TLS.

Upozornění: Předchozí příkazy AT-TLS jsou pouze minimální konfigurací. Existují další příkazy zásad AT-TLS s AT-TLS, které zde nejsou dokumentovány, a v závislosti na potřebě je lze použít s produktem IBM MQ . Produkt IBM MQ však byl testován pouze s popsanými zásadami.

Resetování tajných klíčů SSL a TLS

Produkt IBM MQ podporuje resetování tajných klíčů ve správcích front a klientech.

Tajné klíče se resetují, když uvedený počet šifrovaných bajtů dat proudí přes kanál. Pokud jsou povoleny prezenční signály kanálu, tajný klíč se resetuje před odesláním nebo přijetím dat po synchronizačním signálu kanálu.

Hodnota resetování klíče je vždy nastavena inicializační stranou kanálu IBM MQ .

Správce front

Pro správce front použijte příkaz **ALTER QMGR** s parametrem **SSLRKEYC** k nastavení hodnot použitých během opětovného vyjednávání klíče.

IBM i V systému IBM ipoužijte **CHGMQM** s parametrem **SSLRSTCNT** .

Klient MQI

Standardně klienti MQI znovu nevyjednávají tajný klíč. Klienta MQI můžete znovu vyjednat jedním ze tří způsobů. V následujícím seznamu jsou metody zobrazeny v pořadí podle priority. Zadáte-li více hodnot, použije se hodnota nejvyšší priority.

1. Pomocí pole KeyResetPočet ve struktuře MQSCO ve volání MQCONNX.
2. Pomocí proměnné prostředí **MQSSLRESET**.
3. Nastavením atributu **SSLKeyResetCount** v sekci SSL konfiguračního souboru klienta.

Tyto proměnné lze nastavit na celé číslo v rozsahu 0 až 999 999 999, což představuje počet nešifrovaných bajtů odeslaných a přijatých v rámci konverzace TLS před opětovným vyjednáním tajného klíče TLS. Uvedení hodnoty 0 označuje, že tajné klíče TLS nejsou nikdy znovu vyjednány. Zadáte-li počet resetů tajného klíče TLS v rozsahu 1 bajt až 32 kB, budou kanály TLS používat počet resetů tajného klíče 32 kB. Tím se vyvarujte nadměrných resetů klíčů, které by se vyskytly pro malé hodnoty resetu tajného klíče TLS.

Je-li zadána hodnota větší než nula a pro kanál jsou povoleny synchronizační signály kanálu, je tajný klíč také znovu vyjednán před odesláním nebo přijetím dat zprávy po synchronizačním signálu kanálu.

Počet bajtů do doby, než se po každém úspěšném opětném vyjednávání vynuluje další opětné vyjednávání tajného klíče.

Java

V případě systému IBM MQ classes for Javamůže aplikace resetovat tajný klíč jedním z následujících způsobů:

- Nastavením pole Počet sslResetve třídě MQEnvironment.
- Nastavením vlastnosti prostředí MQC.SSL_RESET_COUNT_PROPERTY v objektu hašovací tabulky. Aplikace poté přiřadí hašovací tabulku k poli `properties` ve třídě MQEnvironment nebo předá hašovací tabulku objektu MQQueueManager v konstruktoru.

Pokud aplikace používá více než jeden z těchto způsobů, použijí se obvyklá pravidla pořadí. Pravidla priority viz Třída com.ibm.mq.MQEnvironment .

Hodnota pole sslResetPočet nebo vlastnost prostředí MQC.SSL_RESET_COUNT_PROPERTY představuje celkový počet bajtů odeslaných a přijatých kódem klienta IBM MQ classes for Java před opětovným vyjednáním tajného klíče. Počet odeslaných bajtů je číslo před šifrováním a počet přijatých bajtů je číslo po dešifrování. Počet bajtů také zahrnuje řídicí informace odeslané a přijaté klientem IBM MQ classes for Java .

Pokud je počet resetů nula, což je výchozí hodnota, tajný klíč nebude nikdy znovu vyjednán. Není-li zadána žádná sada CipherSuite , bude počet resetů ignorován.

JMS

Pro systém IBM MQ classes for JMSpředstavuje vlastnost SSLRESETCOUNT celkový počet bajtů odeslaných a přijatých připojením, než bude znovu vyjednán tajný klíč použitý pro šifrování. Počet odeslaných bajtů je číslo před šifrováním a počet přijatých bajtů je číslo po dešifrování. Počet bajtů také zahrnuje řídicí informace odeslané a přijaté produktem IBM MQ classes for JMS. Chcete-li například konfigurovat objekt ConnectionFactory , který lze použít k vytvoření připojení prostřednictvím kanálu MQI

s povoleným zabezpečením TLS s tajným klíčem, který je znovu vyjednán po toku 4 MB dat, zadejte do správce JMSAdmin následující příkaz:

```
ALTER CF(my.cf) SSLRESETCOUNT(4194304)
```

Je-li hodnota SSLRESETCOUNT nula, což je výchozí hodnota, tajný klíč se nikdy znovu nevyjednává. Vlastnost SSLRESETCOUNT je ignorována, pokud není nastaveno SSLCIPHERSUITE.

.NET

Pro .NET nespravované klienty celočíselná vlastnost **SSLKeyResetCount** označuje počet nešifrovaných bajtů odeslaných a přijatých v rámci konverzace TLS, než je znovu vyjednán tajný klíč. Další informace o použití vlastností objektu v části IBM MQ classes for .NETnaleznete v tématu Získání a nastavení hodnot atributů.

Pro klienty spravované produktem .NET třída SSLStream nepodporuje reset/renegotiation tajného klíče. Chcete-li však být konzistentní s ostatními klienty IBM MQ , IBM MQ spravovaný .NET klient umožňuje aplikacím nastavit **SSLKeyResetCount**. Další informace naleznete v tématu Resetování tajného klíče nebo opětné vyjednávání.

XMS .NET

V případě nespravovaných klientů XMS .NET viz téma Zabezpečená připojení ke správci front IBM MQ.

Související odkazy
ALTER QMGR
DISPLAYQMGR
Změna správce front zpráv (CHGMQM)
Zobrazení správce front zpráv (DSPMQM)

Implementace důvěrnosti v uživatelských programech

Zavedení důvěrnosti v bezpečnostních východech

Uživatelské procedury zabezpečení mohou hrát roli ve službě důvěrnosti generováním a distribucí symetrického klíče pro šifrování a dešifrování dat, která procházejí kanálem. Běžná technika k tomu používá technologii PKI.

Jedna uživatelská procedura zabezpečení vygeneruje náhodnou datovou hodnotu, zašifruje ji pomocí veřejného klíče správce front nebo uživatele, který představuje uživatelská procedura zabezpečení partnera, a odešle zašifrovaná data svému partnerovi ve zprávě zabezpečení. Uživatelská procedura zabezpečení partnera dešifruje hodnotu náhodných dat pomocí soukromého klíče správce front nebo uživatele, kterého reprezentuje. Každá uživatelská procedura zabezpečení nyní může použít hodnotu náhodných dat k odvození symetrického klíče nezávisle na druhém pomocí algoritmu, který oba znali. Alternativně mohou jako klíč použít hodnotu náhodných dat.

Pokud první uživatelská procedura zabezpečení neověřila svého partnera v této době, může další zpráva zabezpečení odeslaná partnerem obsahovat očekávanou hodnotu šifrovanou symetrickým klíčem. První uživatelská procedura zabezpečení může nyní ověřit svého partnera tím, že zkontroluje, zda byla uživatelská procedura zabezpečení partnera schopna správně zašifrovat očekávanou hodnotu.

Uživatelské procedury zabezpečení mohou také využít tuto příležitost, aby se dohodly na algoritmu pro šifrování a dešifrování dat, která proudí na kanálu, pokud je k dispozici více než jeden algoritmus pro použití.

Implementace důvěrnosti v ukončeních zpráv

Uživatelská procedura pro zprávy na odesílajícím konci kanálu může šifrovat data aplikace ve zprávě a jiná uživatelská procedura pro zprávy na přijímajícím konci kanálu může dešifrovat data. Z důvodů výkonu se k tomuto účelu obvykle používá algoritmus symetrického klíče. Další informace o tom, jak lze symetrický klíč generovat a distribuovat, viz “Implementace důvěrnosti v uživatelských programech” na stránce 485.

Záhlaví ve zprávě, například záhlaví přenosové fronty, MQXQH, které zahrnuje vložený deskriptor zprávy, nesmí být šifrováno uživatelskou procedurou pro zprávy. Důvodem je, že převod dat záhlaví zpráv probíhá buď po volání uživatelské procedury pro zprávu na odesílajícím konci, nebo před zavoláním uživatelské procedury pro zprávu na přijímajícím konci. Jsou-li záhlaví šifrována, převod dat selže a kanál se zastaví.

Implementace důvěrnosti v odesílaném a přijímaném ukončení

Uživatelské procedury pro odesílání a příjem lze použít k šifrování a dešifrování dat, která proudí kanálem. Jsou vhodnější než uživatelské procedury pro poskytování této služby z následujících důvodů:

- Na kanálu zpráv mohou být záhlaví zpráv šifrována, stejně jako data aplikace ve zprávách.
- Uživatelské procedury pro odesílání a příjem lze použít na kanálech MQI i na kanálech zpráv. Parametry volání MQI mohou obsahovat citlivá data aplikace, která je třeba chránit v průběhu toku kanálu MQI. Proto můžete použít stejné výstupy pro odeslání a příjem na obou druzích kanálů.

Implementace důvěrnosti v uživatelské proceduře rozhraní API a uživatelské proceduře rozhraní API

Data aplikace ve zprávě mohou být šifrována uživatelskou procedurou rozhraní API nebo přechodu rozhraní API, když je zpráva vložena odesílající aplikací a dešifrována druhou uživatelskou procedurou, když je zpráva načtena přijímající aplikací. Z důvodů výkonu se pro tento účel obvykle používá algoritmus symetrického klíče. Avšak na úrovni aplikace, kde si může mnoho uživatelů navzájem posílat zprávy, problém spočívá v tom, jak zajistit, aby zprávu mohl dešifrovat pouze zamýšlený příjemce zprávy. Jedním řešením je použít jiný symetrický klíč pro každou dvojici uživatelů, kteří si navzájem posílají zprávy. Ale toto řešení může být obtížné a časově náročné na správu, zejména pokud uživatelé patří do různých organizací. Standardní způsob řešení tohoto problému je znám jako *digitální obálka* a používá technologii PKI.

Když aplikace vloží zprávu do fronty, rozhraní API nebo uživatelská procedura přechodu rozhraní API vygeneruje náhodný symetrický klíč a použije klíč k zašifrování dat aplikace ve zprávě. Uživatelská procedura zašifruje symetrický klíč s veřejným klíčem zamýšleného příjemce. Poté nahradí data aplikace ve zprávě zašifrovanými daty aplikace a zašifrovaným symetrickým klíčem. Tímto způsobem může symetrický klíč, a tedy i data aplikace, dešifrovat pouze zamýšlený příjemce. Pokud má šifrovaná zpráva více než jeden možný zamýšlený příjemce, může uživatelská procedura šifrovat kopii symetrického klíče pro každý zamýšlený příjemce.

Pokud jsou pro použití k dispozici různé algoritmy pro šifrování a dešifrování dat aplikace, může uživatelská procedura obsahovat název algoritmu, který použila.

z/OS Důvěrnost pro data v klidu na serveru IBM MQ for z/OS se šifrováním datové sady

Produkt IBM MQ for z/OS může data zákazníka a konfigurační data ztvrdnout zápisem dat do datových sad aktivního protokolu, datových sad archivního protokolu, sad stránek, datových sad zaváděcího programu (BSDS) a datových sad sdílených zpráv (SMDS).

Produkt z/OS poskytuje efektivní šifrování datových sad založené na zásadách. IBM MQ for z/OS podporuje z/OS šifrování datové sady pro:

- Datové sady aktivního protokolu; viz poznámka “1” na stránce 487
- Archivovat datové sady protokolu; viz poznámka “2” na stránce 487
- Sady stránek; viz poznámka “1” na stránce 487

- BSDS; viz poznámka “2” na stránce 487
- Datové sady CSQINP*; viz poznámka “2” na stránce 487
- SMDS; viz poznámka “1” na stránce 487

To poskytuje důvěrnost dat, která jsou v klidu, v jednotlivém správci front systému z/OS .

Notes:

1. Z IBM MQ for z/OS 9.2.0, z/OS šifrování datové sady pro aktivní protokoly. sady stránek a SMDS jsou podporovány.
2. Šifrování datových sad pro protokoly archivace, datové sady BSDS a CSQINP* je podporováno ve všech verzích produktu IBM MQ for z/OS.
3. Produkt IBM MQ Advanced Message Security poskytuje alternativní mechanismus ochrany dat v klidu. Kromě toho produkt AMS také chrání data v paměti a za letu

Další informace o šifrování datové sady z/OS naleznete v tématu Použití vylepšení šifrování datové sady z/OS .

Konfigurace šifrování datové sady z/OS je mimo řízení produktu IBM MQ for z/OS. Nastavení šifrování se projeví při vytvoření datové sady.

To znamená, že před použitím nové zásady šifrování datové sady je třeba znovu vytvořit všechny existující datové sady.

Produkt IBM MQ for z/OS může být spuštěn se směsicí šifrovaných a nešifrovaných datových sad, ale standardní konfigurace by zašifrovala všechny nebo žádné z použitých datových sad.

z/OS Přehled kroků pro šifrování datové sady IBM MQ for z/OS

Jak šifrujete datovou sadu IBM MQ for z/OS .

Než začnete

Musíte se ujistit, že jste správně nakonfigurovali šifrování datové sady z/OS ve vašem podniku. Pokud nastavujete šifrování datové sady ve skupině sdílení front, musíte nakonfigurovat šifrování datové sady z/OS pro sdílení dat.

Poznámka: Šifrovaná datová sada z/OS musí být datovou sadou s rozšířeným formátem.

Postup

1. Nastavte šifrovací klíč a `key-label` v souboru RACF , který se má použít k zašifrování datové sady.
2. Vytvořte profil pro `key-label` ve třídě RACF CSFKEYS.
3. Udělte přístup READ k ID uživatele správce front a všem ostatním ID uživatelů, kteří potřebují přístup k šifrovaným datům.

   To může zahrnovat ID uživatelů, která se používají ke spuštění obslužných programů tisku pro datovou sadu. Uživatel, který spouští příkaz CSQUTIL SCOPY, by například musel dešifrovat příslušnou sadu stránek.
4. Přidružte šifrování `key-label` k názvu datové sady.

   To můžete provést pomocí datové třídy SMS nebo segmentu RACF DFP pro název datové sady nebo kvalifikátor vyšší úrovně.

   Můžete také přidružit `key-label` k datové sadě, když je datová sada přidělena.
5. Přejmenujte všechny existující datové sady pomocí příkazu IDCAMS ALTER.
6. Znovu přidělte datovou sadu s příslušnými atributy.
7. Zkopírujte obsah přejmenované datové sady do nové datové sady pomocí IDCAMS REPRO.

   Data jsou zašifrována akcí jejich zkopírování do datové sady.
8. Opakujte kroky “4” na stránce 487 až “6” na stránce 487 pro všechny ostatní datové sady, které je třeba šifrovat.

z/OS Příklad šifrování aktivních protokolů správce front

Následující témata vás provedou procesem povolení šifrování datových sad v existujících aktivních protokolech.

Poznámka: Proces pro ostatní datové sady je podobný procesu pro aktivní protokoly.

V tomto příkladu platí následující:

- Správce front CSQ1 je spuštěn pod uživatelem QMCSQ1a má datové sady aktivního protokolu CSQ1.LOGS.LOGCOPY1.DS001, CSQ1.LOGS.LOGCOPY1.DS002atd.
- Hardwarové a softwarové prostředí je schopné používat šifrování datové sady z/OS .
- RACF se používá jako prostředek SAF
- Správce front byl zastaven.

Proveďte postup v tomto pořadí:

1. “Konfigurace šifrovacího klíče datové sady pro správce front” na stránce 488
2. “Konfigurace šifrování datové sady pro datové sady protokolu” na stránce 488

z/OS Konfigurace šifrovacího klíče datové sady pro správce front

Způsob konfigurace šifrovacího klíče datové sady pro správce front.

Informace o této úloze

Tato úloha je předpokladem pro “Konfigurace šifrování datové sady pro datové sady protokolu” na stránce 488.

Postup

1. Nastavte klíč AES-256 bitového šifrování DATA s popiskem, například CSQ1DSKY, pomocí obslužného programu generátoru klíčů z/OS (KGUP).
2. Definujte profil RACF CSFKEYS pro šifrovací klíč CSQ1DSKY zadáním následujícího příkazu:

   ```
   RDEFINE CSFKEYS CSQ1DSKY UACC(NONE)
   ```

3. Nakonfigurujte segment ICSF profilu tak, aby umožňoval použití klíče jako chráněného klíče, zadáním následujícího příkazu:

   ```
   RALTER CSFKEYS CSQ1DSKY ICSF(SYMCPACFWRAP(YES) SYMCPACFRET(YES))
   ```

4. Povolte správci front použití šifrovacího klíče tím, že k profilu povolíte přístup pro čtení QMCSQ1 zadáním následujícího příkazu:

   ```
   PERMIT CSQ1DSKY CLASS(CSFKEYS) ID(QMCSQ1) ACCESS(READ)
   ```

   Poskytněte stejný přístup jakémukoli administrativnímu uživateli, který potřebuje číst nebo zapisovat šifrovanou datovou sadu.
5. Aktualizujte třídu CSFKEYS zadáním následujícího příkazu.

   ```
   SETROPTS RACLIST(CSFKEYS) REFRESH
   ```

Jak pokračovat dále

Nakonfigurujte šifrování datové sady pro datové sady, jak je popsáno v tématu “Konfigurace šifrování datové sady pro datové sady protokolu” na stránce 488

z/OS Konfigurace šifrování datové sady pro datové sady protokolu

Jak nakonfigurujete šifrování v datových sadách protokolu.

Než začnete

Ujistěte se, že jste četli:

Přehled kroků pro šifrování IBM MQ for z/OS datové sadya provedení procedury v “Konfigurace šifrovacího klíče datové sady pro správce front” na stránce 488

Informace o této úloze

Tato metoda používá segment DFP generického profilu RACF , takže můžete použít šifrovací klíč pro všechny nové datové sady, které odpovídají profilu.

Případně můžete nakonfigurovat a použít datovou třídu SMS, nebo lze popisek klíče zadat přímo při přidělování datové sady.

Jak bylo popsáno výše, v tomto příkladu je správce front CSQ1 spuštěn pod uživatelem QMCSQ1a má datové sady aktivního protokolu CSQ1.LOGS.LOGCOPY1.DS001, CSQ1.LOGS.LOGCOPY1.DS002atd.

Postup

1. Vytvořte generický profil, pokud neexistuje, zadáním následujícího příkazu:

   ```
   ADDSD 'CSQ1.LOGS.*' UACC(NONE)
   ```

2. Povolte uživateli správce front pozměnit přístup k profilu zadáním následujícího příkazu:

   ```
   PERMIT 'CSQ1.LOGS.*' ID(QMCSQ1) ACCESS(ALTER)
   ```

   Také povolte odpovídající přístup potřebný pro jakéhokoli administrativního uživatele.

3. Přidejte segment DFP s popiskem šifrovacího klíče zadáním následujícího příkazu:

   ```
   ALTDSD 'CSQ1.LOGS.*' DFP(RESOWNER(QMCSQ1) DATAKEY(CSQ1DSKY))
   ```

   Poznámka: Musíte použít stejný šifrovací klíč, který jste použili v konfiguraci šifrovacího klíče datové sady pro správce front.

4. Aktualizujte generické profily datové sady zadáním následujícího příkazu:

   ```
   SETROPTS GENERIC(DATASET) REFRESH
   ```

5. Přejmenujte každou datovou sadu protokolu na zálohu, pak znovu vytvořte a obnovte data pomocí IDCAMS. Následující fragment JCL převádí CSQ1.LOGS.LOGCOPY1.DS001:

   a) Přejmenovat datovou sadu na zálohu

   ```
   //RENAME   EXEC PGM=IDCAMS,REGION=0M
   //SYSPRINT DD SYSOUT=*
   //SYSIN    DD *
     /*-------------------------------------------------------------*/
     /* RENAME DATASET TO BACKUP                                    */
     /*-------------------------------------------------------------*/
     ALTER 'CSQ1.LOGS.LOGCOPY1.DS001'                  -
           NEWNAME('CSQ1.BAK.LOGS.LOGCOPY1.DS001')
   ```

   b) Předefinujte datovou sadu.

   Nová datová sada bude zašifrována kvůli profilu RACF .

   Poznámka: Nahraďte + + EXTDCLASS + + názvem třídy dat rozšířeného formátu, kterou chcete použít pro datovou sadu.

   ```
   //REDEFINE EXEC PGM=IDCAMS,REGION=0M
   //SYSPRINT DD SYSOUT=*
   //SYSIN    DD *
     /*-------------------------------------------------------------*/
     /* REDEFINE THE DATASET                                        */
     /*-------------------------------------------------------------*/
     DEFINE CLUSTER                                  -
   ```

```
          (NAME(CSQ1.LOGS.LOGCOPY1.DS001)             -
          LINEAR                                      -
          SHAREOPTIONS(2 3)                           -
          MODEL(CSQ1.BAK.LOGS.LOGCOPY1.DS001)         -
          DATACLAS(++EXTDCLASS++))
```

c) Zkopírujte data ze zálohy do znovu vytvořené datové sady.

Tento krok šifruje data:

```
//RESTORE  EXEC PGM=IDCAMS,REGION=0M
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
  /*-------------------------------------------------------------*/
  /* RESTORE DATA INTO ENCRYPTED LOG                             */
  /*-------------------------------------------------------------*/
  REPRO INDATASET(CSQ1.BAK.LOGS.LOGCOPY1.DS001)      -
        OUTDATASET(CSQ1.LOGS.LOGCOPY1.DS001)
```

Jak pokračovat dále

Opakujte krok “5” na stránce 489 pro všechny datové sady aktivního protokolu.

Je vyžadován pouze jeden šifrovací klíč a všechny datové sady lze přidružit ke stejnému popisku klíče.

Restartujte správce front CSQ1. Pomocí výstupu příkazu DISPLAY LOG ověřte, že datové sady protokolu byly šifrovány.

z/OS Aspekty šifrování datové sady z/OS ve skupině sdílení front

Každý správce front ve skupině sdílení front (QSG) musí být schopen číst protokoly, BSDS a sdílené datové sady zpráv (SMDS) všech ostatních správců front v rámci skupiny sdílení front.

To znamená, že každý systém, na kterém může být spuštěn člen skupiny sdílení front, musí splňovat požadavky na šifrování datové sady produktu z/OS a všechny popisky klíčů a šifrovací klíče používané k ochraně datových sad pro každého správce front v rámci skupiny sdílení front musí být k dispozici v každém systému.

Správce front před produktem IBM MQ for z/OS 9.1.4 nemůže přistupovat k datové sadě šifrovaného aktivního protokolu.

Správce front před produktem IBM MQ for z/OS 9.1.5 nemůže přistupovat k zašifrovanému SMDS.

Před použitím šifrování datové sady z/OS byste měli migrovat všechny správce front v rámci skupiny sdílení front alespoň na hodnotu IBM MQ for z/OS 9.1.5.

Pokud je správce front v rámci skupiny sdílení front spuštěn s libovolnou šifrovanou datovou sadou aktivního protokolu a byl spuštěn jiný správce front v rámci skupiny sdílení front, ale nebyl naposledy spuštěn s verzí produktu IBM MQ for z/OS , která podporuje šifrované aktivní protokoly, ukončí se správce front se šifrovaným aktivním protokolem nestandardně s kódem nestandardního ukončení 5C6-00F50033.

Můžete převést QSG pro použití šifrovaných aktivních protokolů a SMDS bez úplného výpadku, pomocí:

1. Postupně probíhá migrace jednotlivých správců front alespoň na hodnotu IBM MQ for z/OS 9.1.5 .
2. Převod aktivních protokolů na šifrované datové sady pro každého správce front. To vyžaduje vypnutí a následné restartování správce front.

   Zároveň je pravděpodobné, že sady stránek a protokoly archivu budou povoleny i pro šifrované datové sady, ale to neovlivní migraci skupiny sdílení front.

   Postup pro převod každé datové sady je popsán v části “Příklad šifrování aktivních protokolů správce front” na stránce 488 .
3. Převod SMDS na šifrované datové sady pro každou jednotlivou strukturu CF postupně pomocí:

   a. Zadáním příkazu RESET SMDS (*) ACCESS (DISABLED) CFSTRUCT (název-struktury) pozastavíte přístup správce front k SMDS.

Všimněte si, že během této doby jsou data ve sdílených frontách přidružených k SMDS dočasně nedostupná.

b. Převod každé datové sady, která tvoří SMDS, na šifrované datové sady pomocí procedury popsané v části “Příklad šifrování aktivních protokolů správce front” na stránce 488.

c. Zadáním příkazu RESET SMDS (*) ACCESS (ENABLED) CFSTRUCT (structure-name) obnovte přístup správce front k SMDS.

Upozornění: Před převodem protokolů byste měli správce front ukončit čistě a v průběhu převodu nemusí být možné provést zotavení struktury prostředku Coupling Facility, protože datové sady aktivního protokolu budou dočasně nedostupné.

z/OS Aspekty zpětné migrace při použití šifrování datové sady z/OS

Při zpětné migraci správce front, který má jednu nebo více šifrovaných datových sad, je třeba vzít v úvahu následující skutečnosti.

Šifrování datové sady z/OS je podporováno na následujících datových sadách IBM MQ for z/OS :

- Datové sady aktivního protokolu
- Datové sady protokolu archivace
- Sady stránek
- BSDS
- SMDS
- Datové sady CSQINP*

Pro datové sady BSDS, protokol archivace nebo CSINP* nejsou k dispozici žádné aspekty zpětné migrace.

Je však třeba vzít v úvahu,

- SMDS
- Sada stránek a
- Aktivní protokol

datové sady, protože jejich použití se šifrováním datových sad z/OS není v produktu IBM MQ for z/OS 9.1.0podporováno, a dřívější verze dlouhodobé podpory.

Před zpětnou migrací je třeba odebrat všechny zásady šifrování pro SMDS, sadu stránek a datové sady aktivního protokolu a dešifrovat data. Tento proces je popsán v části “Odebrání šifrování datové sady z datové sady” na stránce 491.

Upozornění: Pokud je správce front, který má být zpětně migrován, součástí skupiny sdílení front (QSG), přečtěte si nejprve část “Aspekty skupiny sdílení front” na stránce 493 .

Odebrání šifrování datové sady z datové sady

Tento příklad popisuje, jak odebrat šifrování datové sady z datové sady protokolu CSQ1.LOGS.LOGCOPY1.DS001. Můžete použít ekvivalentní proces pro SMDS a sady stránek.

Příklad předpokládá, že:

- RACF je zařízení SAF.
- Správce front, který používá datovou sadu, byl zastaven.
- Popisek šifrovacího klíče byl přidružen ke generickému profilu RACF CSQ1.LOGS.*

Proveďte následující postup:

1. Zkopírujte data z datové sady do záložní datové sady.

   a. Definujte datovou sadu zálohy, která není přidružena k popisku šifrovacího klíče.

Poznámka: Nahraďte + + EXTDCLASS + + názvem třídy dat rozšířeného formátu, kterou chcete použít pro datovou sadu.

```
//DEFINE EXEC PGM=IDCAMS,REGION=0M
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
  /*-------------------------------------------------------------*/
  /* DEFINE UNENCRYPTED DATA SET                                 */
  /*-------------------------------------------------------------*/
  DEFINE CLUSTER                                    -
         (NAME(CSQ1.BAK.LOGS.LOGCOPY1.DS001)        -
         LINEAR                                     -
         SHAREOPTIONS(2 3)                          -
         MODEL(CSQ1.LOGS.LOGCOPY1.DS001)            -
         DATACLAS(++EXTDCLASS++))
/*
```

b. Zkopírujte data z původní datové sady do zálohy. Tento krok dešifruje data.

```
//COPY     EXEC PGM=IDCAMS,REGION=0M
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
  /*-------------------------------------------------------------*/
  /* COPY DATA INTO UNENCRYPTED DATA SET                         */
  /*-------------------------------------------------------------*/
  REPRO INDATASET(CSQ1.LOGS.LOGCOPY1.DS001)          -
        OUTDATASET(CSQ1.BAK.LOGS.LOGCOPY1.DS001)
/*
```

c. Odstranit původní datovou sadu

```
//DELETE   EXEC PGM=IDCAMS,REGION=0M
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
  /*-------------------------------------------------------------*/
  /* DELETE ORIGINAL                                             */
  /*-------------------------------------------------------------*/
  DELETE ('CSQ1.LOGS.LOGCOPY1.DS001')
/*
```

d. Přejmenujte zálohu na původní název datové sady. Data zůstávají nezašifrovaná

```
//RENAME   EXEC PGM=IDCAMS,REGION=0M
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
  /*-------------------------------------------------------------*/
  /* RENAME UNENCRYPTED DATA SET                                 */
  /*-------------------------------------------------------------*/
  ALTER CSQ1.BAK.LOGS.LOGCOPY1.DS001'                -
         NEWNAME('CSQ1.LOGS.LOGCOPY1.DS001)
  ALTER 'CSQ1.BAK.LOGS.LOGCOPY1.DS001.*'              -
         NEWNAME('CSQ1.LOGS.LOGCOPY1.DS001.*')
/*
```

2. Volitelně zopakujte tento proces pro další datové sady, které mají přidružený popisek šifrovacího klíče prostřednictvím CSQ1.LOGS.* generický profil.
3. Volitelně, pokud jsou všechny datové sady přidružené k CSQ1.LOGS.* generický profil byl dešifrován, odeberte DATAKEY související s generickým profilem zadáním následujícího příkazu

```
ALTDSD 'CSQ1.LOGS.*' DFP(RESOWNER(QMCSQ1) DATAKEY(CSQ1DSKY))
```

4. Aktualizujte generické profily datové sady zadáním následujícího příkazu:

```
SETROPTS GENERIC(DATASET) REFRESH
```

5. Restartujte správce front.
6. Pokud již šifrovací klíč nepotřebujete, odstraňte jej a odstraňte jeho přidružený profil RACF ze třídy CSFKEYS.

Aspekty skupiny sdílení front

Pokud bude správce front, který je součástí skupiny sdílení front, zpětně migrován na verzi produktu IBM MQ for z/OS , která nepodporuje šifrování datové sady, pak všechny datové sady aktivního protokolu a SMDS všech správců front v rámci skupiny sdílení front musí mít odebrány své zásady šifrování datové sady a jejich data musí být dešifrována.

To platí bez ohledu na to, zda je jeden člen skupiny sdílení front zpětně migrován, nebo všichni členové skupiny sdílení front.

Můžete dosáhnout odebrání zásad šifrování a dešifrování dat bez úplného výpadku QSG:

1. Postupně probíhá ukončování práce jednotlivých správců front v rámci skupiny sdílení front, odebírání zásad šifrování a dešifrování dat z aktivních protokolů pomocí procesu popsaného v tématu “Odebrání šifrování datové sady z datové sady” na stránce 491.

   Pokud má být správce front zpětně migrován, jeho sada stránek by měla být v tuto chvíli také dešifrována. Poté restartujte správce front.
2. Odebrání zásad šifrování a dešifrování dat pro SMDS jednotlivých struktur prostředku CF postupně pomocí:
   a. Zadání příkazu

      ```
      RESET SMDS(*) ACCESS(DISABLED) CFSTRUCT(structure-name)
      ```

      chcete-li pozastavit přístup správce front k SMDS. Během této doby budou data ve sdílených frontách přidružených k SMDS dočasně nedostupná.
   b. Postupujte podle procesu v souboru “Odebrání šifrování datové sady z datové sady” na stránce 491 pro každou datovou sadu, která tvoří SMDS.
   c. Zadání příkazu

      ```
      RESET SMDS(*) ACCESS(ENABLED) CFSTRUCT(structure-name)
      ```

      chcete-li obnovit přístup správce front k SMDS.

Použití šifrování datové sady z/OS se správcem front, který ji nepodporuje

Pokud omylem provedete zpětnou migraci správce front na verzi produktu IBM MQ for z/OS , která nepodporuje šifrování datové sady, a zapomenete odebrat zásady šifrování a dešifrovat data, která obdržíte při pokusu správce front o přístup k datové sadě.

Chyba závisí na typu datové sady a je uvedena v následující tabulce.

Poznámka: Pokud se vyskytne jedna nebo více těchto chyb, musíte postupovat podle procesů popsaných v části “Odebrání šifrování datové sady z datové sady” na stránce 491 pro ovlivněnou datovou sadu. Ty lze provést bez změny verze produktu IBM MQ for z/OS.

Datová sada	Chyba, pokud správce front nepodporuje šifrování datové sady z/OS
Sada stránek 0	Neukončit 5C6-00C91400 při spuštění správce front
Sady stránek 1-99	MQRC 2193 "Chyba sady stránek" při přístupu k sadě stránek, například na MQPUT
Aktivní protokol	Nestandardně ukončit 5C6-00E80084 při spuštění správce front
SMDS	Zpráva IEC161I-122 byla zaprotokolována. "Datová sada má KEYLABEL, ale uživatel neurčil, že by aplikace mohla zpracovat šifrování." SMDS označeno jako AVAIL (ERROR).

Integrita dat zpráv

Chcete-li zachovat integritu dat, můžete použít různé typy uživatelského programu k poskytnutí výtahu zpráv nebo digitálních podpisů pro vaše zprávy.

Integrita dat

Implementace integrity dat ve zprávách

Při použití protokolu TLS určuje vaše volba CipherSpec úroveň integrity dat v podniku. Používáte-li službu IBM MQ Advanced Message Service (AMS), můžete určit integritu pro jedinečnou zprávu.

Implementace integrity dat v uživatelských procedur zpráv

Zpráva může být digitálně podepsána uživatelskou procedurou pro zprávy na odesílajícím konci kanálu. Digitální podpis pak může být zkontrolován uživatelskou procedurou pro zprávy na přijímacím konci kanálu, aby se zjistilo, zda byla zpráva záměrně upravena.

Určitou ochranu lze poskytnout pomocí kódu digest zprávy namísto digitálního podpisu. Kód digest zprávy může být účinný proti příležitostným nebo nevybíravým manipulacím, ale nebrání informovanější osobě ve změně nebo nahrazení zprávy a generování zcela nového kódu digest pro ni. To platí zejména v případě, že algoritmus používaný ke generování kódu digest zprávy je dobře známý.

Implementace integrity dat v odesílaném a přijímaném ukončení

V kanálu zpráv jsou uživatelské procedury zpráv vhodnější pro poskytování této služby, protože uživatelská procedura zpráv má přístup k celé zprávě. V kanálu MQI mohou parametry volání MQI obsahovat data aplikace, která je třeba chránit, a tuto ochranu mohou poskytnout pouze uživatelské procedury pro odesílání a příjem.

Implementace integrity dat v uživatelské proceduře rozhraní API nebo uživatelské proceduře rozhraní API

Zpráva může být digitálně podepsána uživatelskou procedurou rozhraní API nebo přechodem přes rozhraní API, když je zpráva vložena odesílající aplikací. Digitální podpis pak může být zkontrolován druhou uživatelskou procedurou, když je zpráva načtena přijímající aplikací, aby se zjistilo, zda byla zpráva záměrně upravena.

Určitou ochranu lze poskytnout pomocí kódu digest zprávy namísto digitálního podpisu. Kód digest zprávy může být účinný proti příležitostným nebo nevybíravým manipulacím, ale nebrání informovanější osobě ve změně nebo nahrazení zprávy a generování zcela nového kódu digest pro ni. To platí zejména v případě, že algoritmus používaný ke generování kódu digest zprávy je dobře známý,

Další informace

Další informace o zajištění integrity dat naleznete v části “Povolení CipherSpecs” na stránce 438 .

Související úlohy

Připojení dvou správců front pomocí protokolu TLS

Bezpečné připojení klienta ke správci front

Auditování

Pomocí zpráv událostí můžete zkontrolovat narušení zabezpečení nebo pokusy o narušení. Můžete také zkontrolovat zabezpečení systému pomocí konzoly IBM MQ Explorer.

Chcete-li zjistit pokusy o provedení neautorizovaných akcí, jako je připojení ke správci front nebo vložení zprávy do fronty, zkontrolujte zprávy událostí vytvořené vašimi správci front, zejména zprávy událostí oprávnění. Další informace o zprávách událostí správce front naleznete v tématu Události správce fronta další informace o monitorování událostí obecně naleznete v tématu Monitorování událostí.

Zachování zabezpečení klastrů

Autorizujte nebo zabraňte správcům front, kteří se připojují ke klastrům nebo vkládají zprávy do front klastrů. Vynutit, aby správce front opustil klastr. Při konfiguraci protokolu TLS pro klastry vezměte v úvahu některé další aspekty.

Zastavení neautorizovaných správců front odesílajících zprávy

Zabránit neoprávněným správcům front v odesílání zpráv správci front pomocí uživatelské procedury zabezpečení kanálu.

Než začnete

Klastrování nemá žádný vliv na způsob ukončení práce zabezpečení. Přístup ke správci front můžete omezit stejným způsobem jako v prostředí distribuovaných front.

Informace o této úloze

Zabránit vybraným správcům front v odesílání zpráv do správce front:

Postup

1. Definujte uživatelský program zabezpečení kanálu v definici kanálu CLUSRCVR .
2. Napište program, který ověřuje správce front při pokusu o odeslání zpráv v přijímacím kanálu klastru a odepře jim přístup, pokud nejsou autorizováni.

Jak pokračovat dále

Uživatelské programy zabezpečení kanálu jsou volány při inicializaci a ukončení MCA.

Zastavení neautorizovaných správců front vkládající zprávy do front

Pomocí atributu oprávnění vložení kanálu v přijímacím kanálu klastru zastavte neautorizované správce front vkládající zprávy do front. Autorizujte vzdáleného správce front kontrolou ID uživatele ve zprávě pomocí RACF on z/OSnebo OAM na jiných platformách.

Informace o této úloze

K řízení přístupu k frontám použijte prostředky zabezpečení platformy a mechanizmus řízení přístupu v produktu IBM MQ .

Postup

1. Chcete-li zabránit určitým správcům front v vkládání zpráv do fronty, použijte prostředky zabezpečení dostupné na vaší platformě.

   Příklad:

   - RACF nebo jiní externí správci zabezpečení na systému IBM MQ for z/OS
   - Správce oprávnění k objektu (OAM) na jiných platformách.
2. Použijte atribut PUTAUTs oprávněním vložení pro definici kanálu CLUSRCVR .

   Atribut PUTAUT vám umožňuje určit, které identifikátory uživatelů se mají použít k zavedení oprávnění pro vložení zprávy do fronty.

   Volby v atributu PUTAUT jsou:

   DEF
   Použijte výchozí ID uživatele. V systému z/OSmůže kontrola zahrnovat jak ID uživatele přijaté ze sítě, tak ID uživatele odvozené od MCAUSER.

CTX
Použijte ID uživatele v informacích o kontextu přidružených ke zprávě. V systému z/OS může kontrola zahrnovat buď použití ID uživatele přijatého ze sítě, nebo ID odvozeného od MCAUSER, nebo obojí. Tuto volbu použijte, pokud je odkaz důvěryhodný a ověřený.

ONLYMCA (pouze z/OS)
Stejně jako v případě DEF, ale žádné ID uživatele přijaté ze sítě se nepoužívá. Tuto volbu použijte v případě, že odkaz není důvěryhodný. Chcete na něm povolit pouze specifickou sadu akcí, které jsou definovány pro MCAUSER.

ALTMCA (pouze z/OS)
Stejně jako v případě CTXse nepoužívá žádné ID uživatele přijaté ze sítě.

Autorizace vkládání zpráv do front vzdáleného klastru

V systému z/OS nastavte autorizaci pro vložení do fronty klastru pomocí RACF. Na jiných platformách autorizujte přístup pro připojení ke správcům front a pro vkládání do front v těchto správcích front.

Informace o této úloze

Výchozí chování je provádět řízení přístupu vůči serveru SYSTEM.CLUSTER.TRANSMIT.QUEUE. Všimněte si, že toto chování platí i v případě, že používáte více přenosových front.

Specifické chování popsané v tomto tématu platí pouze v případě, že jste nakonfigurovali atribut **ClusterQueueAccessControl** v souboru qm.ini na hodnotu *RQMName*, jak je popsáno v tématu Sekce zabezpečení , a restartovali správce front.

Procedura

- Pro systém z/OSzadejte následující příkazy:

```
RDEFINE MQQUEUE QMgrName.QUEUE. QueueName UACC(NONE)
PERMIT QMgrName.QUEUE. QueueName CLASS(MQADMIN) ID(GroupName) ACCESS(UPDATE)
```

- V systémech AIX, Linux, and Windows zadejte následující příkazy:

```
setmqaut -m QMgrName -t qmgr -g GroupName +connect
setmqaut -m QMgrName -t queue -n QueueName -g GroupName -all +put
```

- Pro systém IBM izadejte následující příkazy:

```
GRTMQMAUT OBJ(' QMgrName ') OBJTYPE(*MQM) USER(GroupName) AUT(*CONNECT)
GRTMQMAUT OBJ(' QueueName ') OBJTYPE(*Q) USER(GroupName) AUT(*PUT) MQMNAME(' QMgrName ')
```

Uživatel může vkládat zprávy pouze do uvedené fronty klastru a žádné jiné fronty klastru.

Názvy proměnných mají následující význam:

QMgrName
Název správce front. V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.

GroupName
Název skupiny, které má být udělen přístup.

QueueName
Název fronty nebo generického profilu, pro který se mají změnit autorizace.

Jak pokračovat dále

Zadáte-li frontu pro odpověď při vložení zprávy do fronty klastru, musí mít přijímající aplikace oprávnění k odeslání odpovědi. Nastavte toto oprávnění podle pokynů v části “Udělení oprávnění pro vložení zpráv do fronty vzdáleného klastru” na stránce 415.

Související pojmy

Sekce zabezpečení v souboru qm.ini

Zabránění připojení správců front ke klastru

Pokud se nepoctivý správce front připojí ke klastru, je obtížné zabránit tomu, aby přijímal zprávy, které nechcete, aby přijímal.

Postup

Chcete-li zajistit, aby se ke klastru připojili pouze určití autorizovaní správci front, máte na výběr ze tří technik:

- Pomocí záznamů ověřování kanálu můžete blokovat připojení kanálu klastru na základě: adresy IP vzdáleného systému, názvu vzdáleného správce front nebo rozlišujícího názvu TLS poskytnutého vzdáleným systémem.
- Chcete-li zabránit neoprávněným správcům front v zápisu do adresáře SYSTEM.CLUSTER.COMMAND.QUEUE, napište uživatelský program. Neomezujte přístup k produktu SYSTEM.CLUSTER.COMMAND.QUEUE tak, aby do něj nemůže zapisovat žádný správce front, nebo byste zabránili jakémukoli správci front v připojení ke klastru.
- Program uživatelské procedury zabezpečení na definici kanálu CLUSRCVR .

Uživatelské procedury zabezpečení na kanálech klastru

Další aspekty při použití uživatelských procedur zabezpečení na kanálech klastru.

Informace o této úloze

Když je kanál odesilatele klastru poprvé spuštěn, používá atributy definované ručně administrátorem systému. Když je kanál zastaven a restartován, vyzvedne atributy z odpovídající definice přijímacího kanálu klastru. Původní definice odesílacího kanálu klastru je přepsána novými atributy, včetně atributu SecurityExit .

Postup

1. Je třeba definovat uživatelskou proceduru pro zabezpečení zprávy na straně odesílatele klastru i na straně příjemce klastru kanálu.

   Počáteční připojení musí být provedeno s výměnou potvrzení o ukončení zabezpečení, i když je název uživatelské procedury zabezpečení odeslán z definice příjemce klastru.
2. Ověřte PartnerName ve struktuře MQCXP v uživatelské proceduře pro zabezpečení zprávy.

   Uživatelská procedura musí umožnit spuštění kanálu pouze v případě, že je autorizován partnerský správce front.
3. Navrhněte uživatelskou proceduru zabezpečení na definici přijímače klastru, aby byla inicializována jako příjemce.
4. Pokud jej navrhnete jako iniciovaného odesilatele, může se neautorizovaný správce front bez uživatelské procedury pro zabezpečení připojit ke klastru, protože nejsou provedeny žádné kontroly zabezpečení.

   Dokud nebude kanál zastaven a restartován, bude možné název SCYEXIT odeslat z definice příjemce klastru a provést úplné kontroly zabezpečení.
5. Chcete-li zobrazit definici odesílacího kanálu klastru, která se momentálně používá, použijte příkaz:

   ```
   DISPLAY CLUSQMGR( queue manager ) ALL
   ```

   Příkaz zobrazí atributy, které byly odeslány z definice příjemce klastru.
6. Chcete-li zobrazit původní definici, použijte příkaz:

```
DISPLAY CHANNEL( channel name ) ALL
```

7. Je možné, že budete muset definovat uživatelskou proceduru automatické definice kanálu CHADEXITve správci front odesilatele klastru, pokud jsou správci front na různých platformách.

   Pomocí uživatelské procedury automatické definice kanálu nastavte atribut SecurityExit na odpovídající formát pro cílovou platformu.
8. Implementujte a nakonfigurujte uživatelskou proceduru zabezpečení.

   z/OS **z/OS**

   Zaváděcí modul uživatelské procedury zabezpečení musí být v datové sadě určené v příkazu CSQXLIB DD procedury adresního prostoru inicializátoru kanálu.

   ALW **Systémy AIX, Linux, and Windows**

   - Knihovna dynamického propojení procedury zabezpečení musí být v cestě uvedené v atributu SCYEXIT definice kanálu.
   - Knihovna dynamického propojení uživatelské procedury automatické definice kanálu musí být v cestě uvedené v atributu CHADEXIT definice správce front.

Vynucení opuštění klastru nežádoucími správci front

Vynuťte, aby nechtěný správce front opustil klastr, zadáním příkazu RESET CLUSTER ve správci front úplného úložiště.

Informace o této úloze

Můžete vynutit, aby nechtěný správce front opustil klastr. Pokud je například odstraněn správce front, ale jeho přijímací kanály klastru jsou pro klastr stále definovány. Možná budete chtít uklidit.

Pouze správci front úplného úložiště jsou autorizováni k vysunutí správce front z klastru.

Poznámka: Ačkoli použití příkazu RESET CLUSTER vynutí odebrání správce front z klastru, použití příkazu RESET CLUSTER samo o sobě nebrání opětovnému připojení správce front ke klastru později. Chcete-li se ujistit, že se správce front znovu nepřipojí ke klastru, postupujte podle pokynů v části “Zabránění připojení správců front ke klastru” na stránce 497.

Chcete-li vysunout správce front OSLO z klastru NORWAY, postupujte takto:

Postup

1. Ve správci front úplného úložiště zadejte příkaz:

```
RESET CLUSTER(NORWAY) QMNAME(OSLO) ACTION(FORCEREMOVE)
```

2. Alternativně použijte QMID místo QMNAME v příkazu:

```
RESET CLUSTER(NORWAY) QMID(qmid) ACTION(FORCEREMOVE)
```

   Poznámka: QMID je řetězec, takže hodnota qmid by měla být uzavřena v apostrofech, například QMID('FR01_2019-07-15_14.42.42').

Výsledky

Vynucené odebrání správce front se nezmění; jeho definice lokálního klastru ukazují, že je v klastru. Definice ve všech ostatních správcích front ji v klastru nezobrazují.

Zabránění správcům front v přijímání zpráv

Správci front klastru můžete zabránit v přijímání zpráv, které nemá oprávnění přijímat, pomocí uživatelských programů.

Informace o této úloze

Je obtížné zastavit správce front, který je členem klastru, v definování fronty. Existuje nebezpečí, že se nepoctivý správce front připojí ke klastru a definuje vlastní instanci jedné z front v klastru. Nyní může přijímat zprávy, které nemá oprávnění přijímat. Chcete-li zabránit tomu, aby správce front přijímal zprávy, použijte jednu z následujících voleb uvedených v proceduře.

Procedura

- Uživatelský program kanálu na každém odesílacím kanálu klastru. Uživatelský program používá název připojení k určení vhodnosti cílového správce front pro odesílání zpráv.
- Uživatelský program pracovní zátěže klastru, který pomocí cílových záznamů určuje vhodnost cílové fronty a správce front pro odesílání zpráv.

SSL/TLS a klastry

Při konfiguraci protokolu TLS pro klastry je definice kanálu CLUSRCVR šířena do jiných správců front jako automaticky definovaný kanál CLUSSDR. Pokud kanál CLUSRCVR používá protokol TLS, je třeba konfigurovat protokol TLS pro všechny správce front, kteří prostřednictvím kanálu komunikují.

Další informace o protokolu TLS viz “Protokoly zabezpečení TLS v adresáři IBM MQ” na stránce 24. Rada je obecně použitelná pro kanály klastru, ale možná budete chtít věnovat zvláštní pozornost následujícímu:

V klastru IBM MQ je konkrétní definice kanálu CLUSRCVR často šířena do mnoha dalších správců front, kde je transformována na automaticky definovanou CLUSSDR. Následně se automaticky definovaný soubor CLUSSDR použije ke spuštění kanálu na server CLUSRCVR. Pokud je CLUSRCVR nakonfigurován pro konektivitu TLS, platí následující aspekty:

- Všichni správci front, kteří chtějí komunikovat s tímto produktem CLUSRCVR , musí mít přístup k podpoře TLS. Toto ustanovení TLS musí podporovat specifikaci CipherSpec pro kanál.
- Různí správci front, do kterých byly automaticky definované odesílací kanály klastru šířeny, budou mít každý přiřazen jiný rozlišující název. Má-li být na serveru CLUSRCVR použita kontrola typu peer s rozlišujícími názvy, musí být nastavena tak, aby se všechny rozlišující názvy, které lze přijmout, úspěšně shodovaly.

  Předpokládejme například, že všichni správci front, kteří budou hostiteli odesílacích kanálů klastru, jež se budou připojovat ke konkrétnímu serveru CLUSRCVR, mají přiřazeny certifikáty. Předpokládejme také, že rozlišující názvy ve všech těchto certifikátech definují zemi jako Spojené království, organizaci jako IBM, organizační jednotku jako IBM MQ Vývoj a všechny mají společné názvy ve tvaru DEVT.QMnnn, kde nnn je číselné.

  V tomto případě hodnota SSLPEER `C=UK, O=IBM, OU=IBM MQ Development, CN=DEVT.QM*` na CLUSRCVR umožní úspěšné připojení všech požadovaných odesílacích kanálů klastru, ale zabrání nežádoucím odesílacím kanálům klastru v připojení.
- Pokud jsou použity vlastní řetězce CipherSpec , mějte na paměti, že vlastní formáty řetězců nejsou povoleny na všech platformách. Příkladem toho je, že řetězec CipherSpec RC4_SHA_US má hodnotu 05 na systému IBM i , ale není platnou specifikací na systémech AIX, Linux, and Windows . Pokud jsou tedy vlastní parametry SSLCIPH použity na serveru CLUSRCVR, všechny výsledné automaticky definované odesílací kanály klastru by měly být umístěny na platformách, na kterých základní podpora TLS implementuje tuto specifikaci CipherSpec a na kterých ji lze zadat s vlastní hodnotou. Pokud nemůžete vybrat hodnotu parametru SSLCIPH , která bude pochopena v celém klastru, budete potřebovat uživatelskou proceduru automatické definice kanálu, abyste ji změnili na něco, čemu budou rozumět používané platformy. Použijte textové řetězce CipherSpec , kde je to možné (například TLS_RSA_WITH_AES_128_CBC_SHA).

Parametr SSLCRLNL se vztahuje na jednotlivého správce front a není šířen do jiných správců front v rámci klastru.

Upgrade klastrovaných správců front a kanálů na SSL/TLS

Proveďte upgrade kanálů klastru jeden po druhém a změňte všechny kanály CLUSRCVR před kanály CLUSSDR .

Než začnete

Zvažte následující aspekty, protože mohou ovlivnit volbu CipherSpec pro klastr:

- Některé specifikace CipherSpecs nejsou k dispozici na všech platformách. Dávejte pozor na volbu CipherSpec , kterou podporují všichni správci front v klastru.
- Některé specifikace CipherSpecs mohou být v aktuální verzi produktu IBM MQ nové a ve starších verzích nejsou podporovány. Klastr obsahující správce front spuštěné v různých verzích produktu MQ může používat pouze specifikace CipherSpecs podporované jednotlivými verzemi.

  Chcete-li použít novou specifikaci CipherSpec v rámci klastru, musíte nejprve migrovat všechny správce front klastru na aktuální verzi.
- Některé CipherSpecs vyžadují použití specifického typu digitálního certifikátu, zejména těch, které používají šifrování Elliptic Curve Cryptography.

  Upozornění: U správců front, které chcete spojit jako součást klastru, není možné použít kombinaci certifikátů podepsaných pomocí eliptické křivky a certifikátů podepsaných pomocí RSA.

  Všichni správci front v klastru musí používat certifikáty podepsané RSA nebo všechny certifikáty podepsané EC, nikoli kombinaci obojího.

  Další informace viz “Digitální certifikáty a kompatibilita CipherSpec v produktu IBM MQ” na stránce 46.

Upgradujte všechny správce front v klastru na verzi IBM MQ V8 nebo vyšší, pokud ještě nejsou na těchto úrovních. Distribuujte certifikáty a klíče tak, aby TLS fungoval z každého z nich.

Chcete-li provést upgrade na alias CipherSpecs (ANY_TLS13, ANY_TLS13_OR_HIGHER, ANY_TLS12, ANY_TLS12_OR_HIGHERatd.), musíte upgradovat všechny správce front IBM MQ for Multiplatforms v klastru na verzi IBM MQ 9.1.4 nebo vyšší a všechny správce front IBM MQ for z/OS v klastru na verzi IBM MQ for z/OS 9.2.0 nebo novější.

Informace o této úloze

Změňte kanály CLUSRCVR před kanály CLUSSDR .

Postup

1. Přepněte kanály CLUSRCVR na TLS v libovolném pořadí, v jakém se vám líbí, a změňte jeden CLUSRCVR v daném okamžiku a umožněte, aby změny protékají klastrem před změnou dalšího.

   Důležité: Ujistěte se, že neměníte reverzní cestu, dokud nebudou změny pro aktuální kanál distribuovány v rámci klastru.
2. Volitelné: Přepněte všechny ruční kanály CLUSSDR na TLS.

   To nemá žádný vliv na činnost klastru, pokud nepoužijete příkaz REFRESH CLUSTER s volbou REPOS(YES) .

   Poznámka: V případě velkých klastrů může být použití příkazu **REFRESH CLUSTER** pro probíhající klastr s přerušením a poté znovu ve 27 denních intervalech, když objekty klastru automaticky odesílají aktualizace stavu všem zainteresovaným správcům front. Viz téma Aktualizace velkých klastrů mohou ovlivnit jejich výkon a dostupnost.
3. Pomocí příkazu DISPLAY CLUSQMGR se ujistěte, že nová konfigurace zabezpečení byla rozšířena po celém klastru.

4. Restartujte kanály, aby používaly protokol TLS, a spusťte příkaz REFRESH SECURITY (SSL).

Související pojmy

“Povolení CipherSpecs” na stránce 438
Povolte CipherSpec pomocí parametru **SSLCIPH** v příkazu **DEFINE CHANNEL** nebo **ALTER CHANNEL** MQSC.

“Digitální certifikáty a kompatibilita CipherSpec v produktu IBM MQ” na stránce 46
Toto téma poskytuje informace o tom, jak zvolit příslušné specifikace CipherSpecs a digitální certifikáty pro vaši zásadu zabezpečení, a to nastíněním vztahu mezi specifikacemi CipherSpecs a digitálními certifikáty v produktu IBM MQ.

Související informace

Klastrování: Využití doporučených postupů pro příkaz REFRESH CLUSTER

Zakázání SSL/TLS v klastrovaných správcích front a kanálech

Chcete-li vypnout protokol TLS, nastavte parametr SSLCIPH na hodnotu `' '`. Zakažte protokol TLS na kanálech klastru jednotlivě a změňte všechny přijímací kanály klastru před odesílacími kanály klastru.

Informace o této úloze

Změňte jeden přijímací kanál klastru v daném okamžiku a před změnou dalšího povolte, aby změny protékají klastrem.

Důležité: Ujistěte se, že neměníte obrácenou cestu, dokud nebudou změny pro aktuální kanál distribuovány v rámci klastru.

Postup

1. Nastavte hodnotu parametru SSLCIPH na `' '`, prázdný řetězec v apostrofu IBM i nebo `*NONE` v IBM i .

   Protokol TLS můžete na přijímacích kanálech klastru vypnout v libovolném pořadí.

   Všimněte si, že změny proudí v opačném směru přes kanály, na kterých necháte protokol TLS aktivní.
2. Zkontrolujte, zda se nová hodnota odráží ve všech ostatních správcích front pomocí příkazu **DISPLAY CLUSQMGR(*)** ALL.
3. Vypněte protokol TLS na všech odesílacích kanálech ručního klastru.

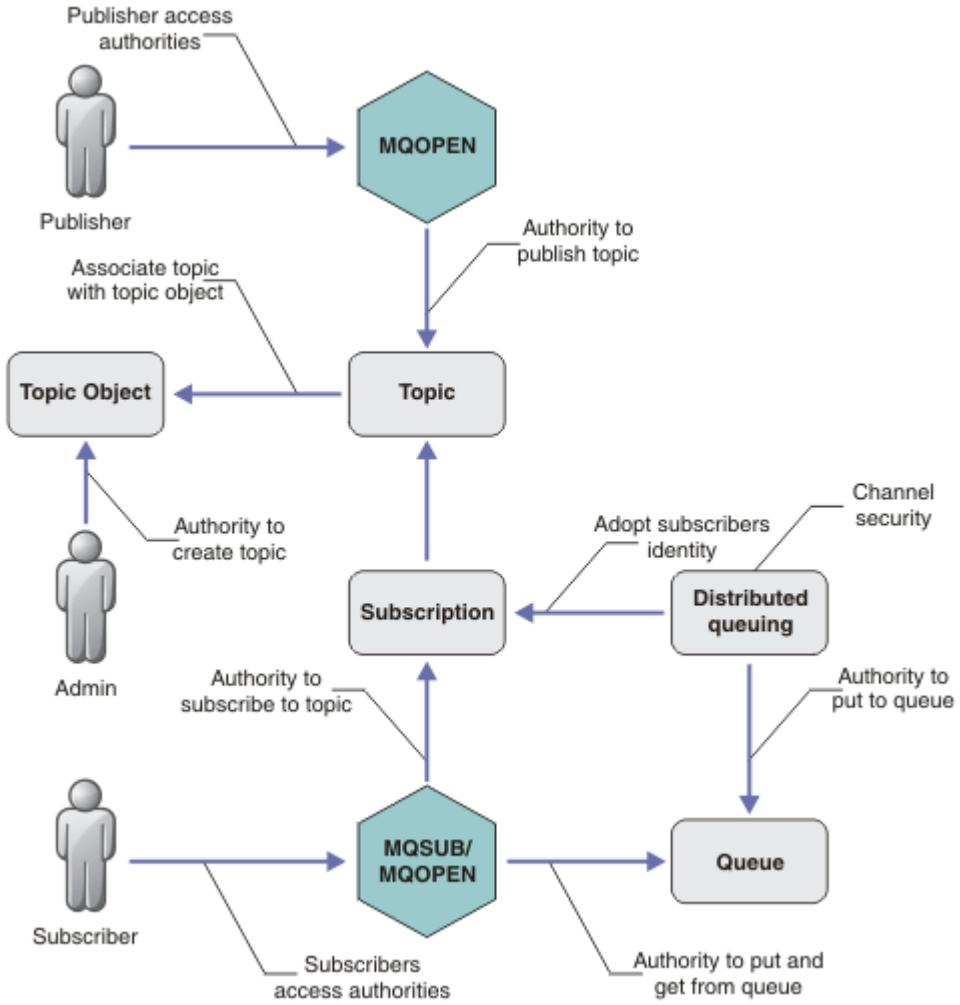
   To nemá žádný vliv na činnost klastru, pokud nepoužijete příkaz **REFRESH CLUSTER** s volbou REPOS (YES) .

   V případě velkých klastrů může být použití příkazu **REFRESH CLUSTER** v průběhu zpracování klastru s přerušením a poté znovu v pravidelných intervalech, když objekty klastru automaticky odesílají aktualizace stavu všem zainteresovaným správcům front. Další informace viz Aktualizace ve velkém klastru může ovlivnit výkon a dostupnost klastru .
4. Zastavte a restartujte odesílací kanály klastru.

Zabezpečení publikování/odběru

Komponenty a interakce, které jsou zapojeny do publikování/odběru, jsou popsány jako úvod k podrobnějším vysvětlením a příkladům, které následují.

Publikování a přihlášení k odběru tématu zahrnuje řadu komponent. Některé vztahy zabezpečení mezi nimi jsou ilustrovány v souboru Obrázek 22 na stránce 502 a popsány v následujícím příkladu.



Obrázek 22. Vztahy zabezpečení publikování/odběru mezi různými komponentami

Témata

Témata jsou identifikována pomocí řetězců témat a jsou obvykle uspořádána do stromů, viz Stromy témat. Musíte přidružit téma k objektu tématu, abyste mohli řídit přístup k tématu. “Model zabezpečení tématu” na stránce 504 vysvětluje, jak zabezpečit témata pomocí objektů témat.

Objekty administrativních témat

Pomocí příkazu **setmqaut** se seznamem objektů administrativních témat můžete řídit, kdo má přístup k tématu a za jakým účelem. Viz příklady, “Udělit uživateli přístup k odběru tématu” na stránce 508 a “Udělit uživateli přístup pro publikování v tématu” na stránce 515. z/OS Řízení přístupu k objektům témat v systému z/OSnaleznete v tématu Profily pro zabezpečení témat.

Odběry

Přihlaste se k odběru jednoho nebo více témat vytvořením odběru s dodáním řetězce tématu, který může obsahovat zástupné znaky, aby se shodoval s řetězci tématu publikování. Další podrobnosti viz:

Přihlásit se k odběru pomocí objektu tématu

“Přihlášení k odběru pomocí názvu objektu tématu” na stránce 505

Přihlásit se k odběru pomocí tématu

“Přihlášení k odběru pomocí řetězce tématu, kde uzel tématu neexistuje” na stránce 506

Přihlásit se k odběru pomocí tématu se zástupnými znaky

“Přihlášení k odběru pomocí řetězce tématu, který obsahuje zástupné znaky” na stránce 506

Odběr obsahuje informace o identitě odběratele a identitě cílové fronty, do které mají být publikování umístěna. Obsahuje také informace o tom, jak má být publikování umístěno do cílové fronty.

Kromě definování, kteří odběratelé mají oprávnění k odběru určitých témat, můžete omezit odběry na použití jednotlivými odběrateli. Můžete také řídit, jaké informace o odběrateli bude správce front používat při umisťování publikací do cílové fronty. Viz "Zabezpečení odběru" na stránce 521.

Fronty

Cílová fronta je důležitá pro zabezpečení. Je lokální vzhledem k odběrateli a publikování, která odpovídají odběru, jsou na něj umístěna. Je třeba zvážit přístup k cílové frontě ze dvou perspektiv:

1. Vložení publikování do cílové fronty.
2. Probíhá získávání publikování z cílové fronty.

Správce front vloží publikování do cílové fronty s použitím identity poskytnuté odběratelem. Odběratel nebo program, kterému byla delegována úloha získávání publikací, vezme zprávy z fronty. Viz "Oprávnění k cílovým frontám" na stránce 506.

Neexistují žádné aliasy objektů tématu, ale jako alias pro objekt tématu můžete použít alias fronty. Pokud tak učiníte, stejně jako kontrolu oprávnění k použití tématu pro publikování nebo odběr, správce front zkontroluje oprávnění k použití fronty.

"Zabezpečení publikování/odběru mezi správci front" na stránce 522

Vaše oprávnění k publikování nebo odběru tématu je kontrolováno v lokálním správci front s použitím lokálních identit a autorizací. Autorizace nezávisí na tom, zda je téma definováno či nikoli, ani na tom, kde je definováno. V důsledku toho je třeba při použití klastrovaných témat provést autorizaci tématu pro každého správce front v klastru.

Poznámka: Model zabezpečení pro témata se liší od modelu zabezpečení pro fronty. Stejného výsledku pro fronty lze dosáhnout definováním aliasu fronty lokálně pro každou klastrovanou frontu.

Správci front si vyměňují odběry v klastru. Ve většině konfigurací klastru IBM MQ jsou kanály konfigurovány s použitím produktu PUTAUT=DEF pro umístění zpráv do cílových front s použitím oprávnění procesu kanálu. Můžete upravit konfiguraci kanálu tak, aby používala produkt PUTAUT=CTX a vyžadovala, aby měl odebírající uživatel oprávnění k šíření odběru do jiného správce front v klastru.

"Zabezpečení publikování/odběru mezi správci front" na stránce 522 popisuje, jak změnit definice kanálů tak, aby řídily, kdo může šířit odběry na jiné servery v klastru.

Autorizace

Můžete použít autorizaci na objekty témat, stejně jako na fronty a další objekty. Existují tři operace autorizace, pub, suba `resume` , které můžete použít pouze na témata. Podrobnosti jsou popsány v tématu Určení oprávnění pro různé typy objektů.

Volání funkce

V programech publikování a odběru, jako v programech zařazených do fronty, se kontroly autorizace provádějí při otevírání, vytváření, změně nebo odstraňování objektů. Kontroly se neprovádějí při volání `MQPUT` nebo `MQGET` MQI za účelem vložení a získání publikací.

Chcete-li publikovat téma, proveďte na tématu příkaz `MQOPEN` , který provádí kontroly autorizace. Publikujte zprávy do popisovače tématu pomocí příkazu `MQPUT` , který neprovádí žádné kontroly autorizace.

Chcete-li se přihlásit k odběru tématu, obvykle provedete příkaz `MQSUB` pro vytvoření nebo obnovení odběru a také otevřete cílovou frontu pro příjem publikování. Případně otevřete cílovou frontu pomocí samostatného příkazu `MQOPEN` a poté pomocí příkazu `MQSUB` vytvořte nebo obnovte odběr.

Ať už použijete jakákoli volání, správce front zkontroluje, zda se můžete přihlásit k odběru tématu, a získá výsledná publikování z cílové fronty. Není-li cílová fronta spravována, provede se také kontrola autorizace, zda je správce front schopen umisťovat publikování do cílové fronty. Používá identitu, kterou převzala z odpovídajícího odběru. Předpokládá se, že správce front je vždy schopen umísťovat publikování do spravovaných cílových front.

Role

Uživatelé jsou zapojeni do spouštění aplikací publikování/odběru ve čtyřech rolích:

1. Vydavatel
2. Odběratel
3. Administrátor tématu
4. IBM MQ Administrátor-člen skupiny `mqm`

Definujte skupiny s příslušnými autorizacemi, které odpovídají rolím administrace publikování, odběru a tématu. Poté můžete těmto skupinám přiřadit činitele, kteří je autorizují k provádění specifických úloh publikování a odběru.

Kromě toho je třeba rozšířit oprávnění k administrativním operacím na administrátora front a kanálů odpovědných za přesouvání publikování a odběrů.

Model zabezpečení tématu

Atributy zabezpečení mohou být přidruženy pouze k definovaným objektům témat. Popis objektů témat naleznete v tématu Objekty administrativních témat. Atributy zabezpečení určují, zda je určené ID uživatele nebo skupina zabezpečení povolena k provedení operace odběru nebo publikování pro každý objekt tématu.

Atributy zabezpečení jsou přidruženy k příslušnému uzlu administrace ve stromu témat. Když je provedena kontrola oprávnění pro konkrétní ID uživatele během operace odběru nebo publikování, je udělené oprávnění založeno na atributech zabezpečení přidruženého uzlu stromu témat.

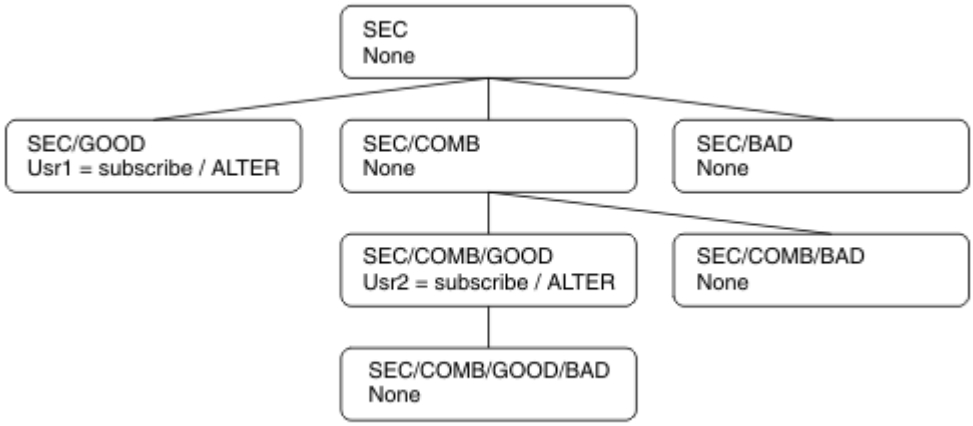
Atributy zabezpečení jsou seznam přístupových práv, který určuje, jaké oprávnění má konkrétní ID uživatele operačního systému nebo skupina zabezpečení k objektu tématu.

Zvažte následující příklad, kde byly objekty tématu definovány se zobrazenými atributy zabezpečení nebo oprávněními:

Tabulka 87. Příklad oprávnění k objektům tématu

Název tématu	Řetězec tématu	Oprávnění-nikoli z/OS	z/OS oprávnění
SECROOT	SEC	Není	Není
SECGOOD	SEC/GOOD	usr1+subscribe	ALTER HLQ.SUBSCRIBE.SECGOOD
SECBAD	SEC/BAD	Není	Není HLQ.SUBSCRIBE.SECBAD
SECCOMB	SEC/COMB	Není	Není HLQ.SUBSCRIBE.SECCOMB
SECCOMBB	SEC/COMB/ GOOD/BAD	Není	Není HLQ.SUBSCRIBE.SECCOMBB
SECCOMBG	SEC/COMB/GOOD	usr2+subscribe	ALTER HLQ.SUBSCRIBE.SECCOMBG
SECCOMBN	SEC/COMB/BAD	Není	Není HLQ.SUBSCRIBE.SECCOMBN

Strom témat s přidruženými atributy zabezpečení na každém uzlu lze znázornit takto:



V uvedených příkladech jsou uvedena následující oprávnění:

- V kořenovém uzlu stromu /SECnemá žádný uživatel oprávnění k tomuto uzlu.
- usr1 bylo uděleno oprávnění k odběru objektu /SEC/GOOD
- usr2 bylo uděleno oprávnění k odběru objektu /SEC/COMB/GOOD

Přihlášení k odběru pomocí názvu objektu tématu

Při přihlášení k odběru objektu tématu zadáním názvu MQCHAR48 je ve stromu témat umístěn odpovídající uzel. Pokud atributy zabezpečení přidružené k uzlu označují, že má uživatel oprávnění k odběru, pak je přístup udělen.

Pokud uživateli není udělen přístup, nadřízený uzel ve stromu určí, zda má uživatel oprávnění přihlásit se k odběru na úrovni nadřízeného uzlu. Pokud ano, pak je přístup udělen. Pokud ne, pak se bere v úvahu nadřízený prvek tohoto uzlu. Rekurze pokračuje, dokud není nalezen uzel, který uděluje uživateli oprávnění k odběru. Rekurze se zastaví, když je kořenový uzel považován za uzel bez uděleného oprávnění. V druhém případě je přístup odepřen.

Stručně řečeno, pokud některý uzel v cestě udělí oprávnění přihlásit se k odběru tohoto uživatele nebo aplikace, může se odběratel přihlásit k odběru na tomto uzlu nebo kdekoli pod tímto uzlem ve stromu témat.

Kořenový uzel v příkladu je SEC.

Uživateli je uděleno oprávnění k odběru, pokud seznam přístupových práv označuje, že vlastní ID uživatele má oprávnění nebo že skupina zabezpečení operačního systému, jejíž je ID uživatele členem, má oprávnění.

Takže například:

- Pokud se produkt usr1 pokusí přihlásit k odběru pomocí řetězce tématu SEC/GOOD, bude odběr povolen, protože ID uživatele má přístup k uzlu přidruženému k tomuto tématu. Pokud se však produkt usr1 pokusil přihlásit k odběru pomocí řetězce tématu SEC/COMB/GOOD , odběr nebude povolen, protože ID uživatele nemá přístup k uzlu, který je k němu přidružen.
- Pokud se produkt usr2 pokusí přihlásit k odběru pomocí řetězce tématu SEC/COMB/GOOD , bude odběr povolen, protože ID uživatele má přístup k uzlu přidruženému k tématu. Pokud se však produkt usr2 pokusil přihlásit k odběru produktu SEC/GOOD , nebude odběr povolen, protože ID uživatele nemá přístup k uzlu, který je k němu přidružen.
- Pokud se produkt usr2 pokusí přihlásit k odběru pomocí řetězce tématu SEC/COMB/GOOD/BAD , bude odběr povolen, protože ID uživatele má přístup k nadřízenému uzlu SEC/COMB/GOOD.
- Pokud se produkt usr1 nebo usr2 pokusí přihlásit k odběru pomocí řetězce tématu /SEC/COMB/BAD, nebude povolen ani jeden z nich, protože nemají přístup k uzlu tématu, který je k němu přidružen, ani k nadřízeným uzlům tohoto tématu.

Operace odběru určující název objektu tématu, který neexistuje, způsobí chybu MQRC_UNKNOWN_OBJECT_NAME.

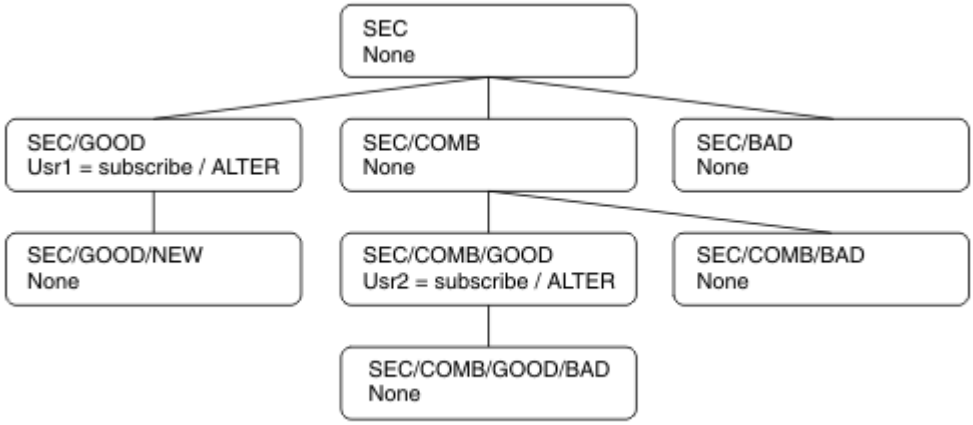
Přihlášení k odběru pomocí řetězce tématu, kde uzel tématu existuje

Chování je stejné jako při zadávání tématu pomocí názvu objektu MQCHAR48 .

Přihlášení k odběru pomocí řetězce tématu, kde uzel tématu neexistuje

Zvažte případ odebírající aplikace a určete řetězec tématu představující uzel tématu, který v současné době ve stromu témat neexistuje. Kontrola oprávnění se provádí podle popisu v předchozí části. Kontrola začíná nadřízeným uzlem toho, který je reprezentován řetězcem tématu. Je-li uděleno oprávnění, bude ve stromu témat vytvořen nový uzel představující řetězec tématu.

Například `usr1` se pokusí přihlásit k odběru tématu `SEC/GOOD/NEW`. Oprávnění je uděleno, protože `usr1` má přístup k nadřízenému uzlu `SEC/GOOD`. Ve stromu se vytvoří nový uzel tématu, jak ukazuje následující diagram. Nový uzel tématu není objektem tématu, k němu nejsou přímo přidruženy žádné atributy zabezpečení; atributy jsou zděděny od jeho nadřízeného prvku.



Přihlášení k odběru pomocí řetězce tématu, který obsahuje zástupné znaky

Zvažte případ přihlášení k odběru pomocí řetězce tématu, který obsahuje zástupný znak. Provede se kontrola oprávnění pro uzel ve stromu témat, který odpovídá úplné části řetězce tématu.

Pokud se tedy aplikace přihlásí k odběru produktu `SEC/COMB/GOOD/*`, provede se kontrola oprávnění, jak je uvedeno v předchozích dvou sekcích na uzlu `SEC/COMB/GOOD` ve stromu témat.

Podobně, pokud se aplikace musí přihlásit k odběru produktu `SEC/COMB/*/GOOD`, provede se kontrola oprávnění na uzlu `SEC/COMB`.

Oprávnění k cílovým frontám

Při přihlášení k odběru tématu je jedním z parametrů popisovač `hobj` fronty, která byla otevřena pro výstup pro příjem publikování.

Není-li parametr `hobj` uveden, ale je prázdný, je spravovaná fronta vytvořena, pokud platí následující podmínky:

- Byla zadána volba `MQSO_MANAGED` .
- Odběr neexistuje.
- Je zadáno vytvoření.

Pokud je hodnota `hobj` prázdná a měníte nebo obnovujete existující odběr, může být dříve poskytnutá cílová fronta spravovaná nebo nespravovaná.

Aplikace nebo uživatel provádějící požadavek MQSUB musí mít oprávnění pro vložení zpráv do cílové fronty, kterou poskytl; v podstatě oprávnění pro vložení publikovaných zpráv do této fronty. Kontrola oprávnění se řídí existujícími pravidly pro kontrolu zabezpečení fronty.

Kontrola zabezpečení zahrnuje alternativní ID uživatele a kontroly zabezpečení kontextu v případě potřeby. Chcete-li mít možnost nastavit libovolné pole kontextu identity, musíte zadat volbu MQSO_SET_IDENTITY_CONTEXT a také volbu MQSO_CREATE nebo MQSO_ALTER . Nemůžete nastavit žádné pole kontextu identity v požadavku MQSO_RESUME .

Pokud je cílem spravovaná fronta, nebudou provedeny žádné kontroly zabezpečení pro spravované místo určení. Máte-li povoleno přihlásit se k odběru tématu, předpokládá se, že můžete používat spravované cíle.

Publikování s použitím názvu tématu nebo řetězce tématu, kde uzel tématu existuje

Model zabezpečení pro publikování je stejný jako pro přihlášení k odběru, s výjimkou zástupných znaků. Publikace neobsahují zástupné znaky, takže neexistuje žádný případ řetězce tématu, který by obsahoval zástupné znaky.

Oprávnění k publikování a odběru jsou odlišná. Uživatel nebo skupina může mít oprávnění provést jednu, aniž by byla nutně schopna provést druhou.

Při publikování do objektu tématu zadáním názvu MQCHAR48 nebo řetězce tématu je ve stromu témat umístěn příslušný uzel. Pokud atributy zabezpečení přidružené k uzlu tématu označují, že má uživatel oprávnění k publikování, pak je přístup udělen.

Pokud není udělen přístup, nadřízený uzel ve stromu určí, zda má uživatel oprávnění k publikování na této úrovni. Pokud ano, pak je přístup udělen. Pokud ne, bude rekurze pokračovat, dokud nebude nalezen uzel, který uživateli udělí oprávnění k publikování. Rekurze se zastaví, když je kořenový uzel považován za uzel bez uděleného oprávnění. V druhém případě je přístup odepřen.

Stručně řečeno, pokud některý uzel v cestě udělí oprávnění k publikování tomuto uživateli nebo aplikaci, může vydavatel publikovat na tomto uzlu nebo kdekoli pod tímto uzlem ve stromu témat.

Publikování s použitím názvu tématu nebo řetězce tématu, kde uzel tématu neexistuje

Stejně jako v případě operace odběru, když aplikace publikuje řetězec tématu představující uzel tématu, který momentálně neexistuje ve stromu témat, provede se kontrola oprávnění počínaje nadřízeným uzlem uzlu představovaným řetězcem tématu. Je-li uděleno oprávnění, bude ve stromu témat vytvořen nový uzel představující řetězec tématu.

Publikování pomocí alias fronty, která se interpretuje na objekt tématu

Pokud publikujete s použitím alias fronty, která se interpretuje jako objekt tématu, dojde ke kontrole zabezpečení jak pro alias frontu, tak pro základní téma, na které se vyhodnocuje.

Kontrola zabezpečení ve frontě aliasů ověřuje, zda má uživatel oprávnění vkládat zprávy do této fronty aliasů, a kontrola zabezpečení v tématu ověřuje, zda může uživatel do tohoto tématu publikovat. Když se alias fronta interpretuje na jinou frontu, kontroly se v základní frontě neprovádějí. Kontrola oprávnění se provádí odlišně pro témata a fronty.

Zavření odběru

Pokud zavřete odběr pomocí volby MQCO_REMOVE_SUB , dojde k další kontrole zabezpečení, pokud jste odběr nevytvořili pod tímto popisovačem.

Provede se kontrola zabezpečení, abyste se ujistili, že k tomu máte správné oprávnění, protože výsledkem akce je odebrání odběru. Pokud atributy zabezpečení přidružené k uzlu tématu označují, že má uživatel oprávnění, pak je přístup udělen. Pokud ne, je nadřízený uzel ve stromu považován za uzel, který určí, zda má uživatel oprávnění k uzavření odběru. Rekurze pokračuje, dokud není uděleno oprávnění nebo dokud není dosažen kořenový uzel.

Definování, změna a odstranění odběru

Při administrativním vytvoření odběru se neprovádějí žádné kontroly zabezpečení odběru, namísto použití požadavku rozhraní API MQSUB . Administrátor již získal toto oprávnění prostřednictvím příkazu.

Provádějí se kontroly zabezpečení, aby se zajistilo, že publikování lze vložit do cílové fronty přidružené k odběru. Kontroly se provádějí stejným způsobem jako u požadavku MQSUB .

ID uživatele, které se používá pro tyto kontroly zabezpečení, závisí na zadaném příkazu. Je-li uveden parametr **SUBUSER** , ovlivní to způsob provedení kontroly, jak je uvedeno v části Tabulka 88 na stránce 508:

Tabulka 88. ID uživatelů použitá pro kontroly zabezpečení pro příkazy

Příkaz	Zadaný SUBUSER a prázdný	Zadaný a dokončený SUBUSER	SUBUSER není uveden
	Použít ID administrátora		Použít ID uživatele z odběru LIKE
	Použít ID administrátora		Použijte ID.DEFAULT.SU uživatele zeB -pokud je systémuprázdný, SYSTEMpoužijte ID administrátora
	Použít ID administrátora		Použít ID uživatele z existujícího odběru

Jedinou kontrolou zabezpečení provedenou při odstraňování odběrů pomocí příkazu DELETE SUB je kontrola zabezpečení příkazu.

Příklad nastavení zabezpečení publikování/odběru

Tento oddíl popisuje scénář, ve kterém je nastaveno řízení přístupu k tématům způsobem, který umožňuje použít řízení zabezpečení podle potřeby.

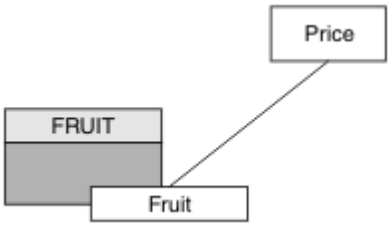
Udělit uživateli přístup k odběru tématu

Toto téma je první v seznamu úloh, které vám sdělí, jak udělit přístup k tématům více než jedním uživatelem.

Informace o této úloze

Tato úloha předpokládá, že neexistují žádné objekty administrativních témat, ani nebyly definovány žádné profily pro odběr nebo publikování. Aplikace vytvářejí nové odběry, nikoli obnovují existující odběry, a používají pouze řetězec tématu.

Aplikace může vytvořit odběr poskytnutím objektu tématu, řetězce tématu nebo kombinace obojího. Bez ohledu na to, jakým způsobem aplikace vybere, bude mít za následek přihlášení k odběru v určitém bodě stromu témat. Pokud je tento bod ve stromu témat reprezentován objektem administrativního tématu, zkontroluje se profil zabezpečení na základě názvu tohoto objektu tématu.



Obrázek 23. Příklad přístupu k objektu tématu

Tabulka 89. Příklad přístupu k objektu tématu		
Téma	**Je vyžadován přístup k odběru**	**Objekt tématu**
Cena	Žádný uživatel	Není
Cena/ovoce	USER1	OVOCE

Definujte nový objekt tématu následujícím způsobem:

Postup

1. Zadejte příkaz MQSC `DEF TOPIC(FRUIT) TOPICSTR('Price/Fruit')`.
2. Udělte přístup následujícím způsobem:

- z/OS **z/OS** :

  Udělte přístup k USER1 pro přihlášení k odběru tématu `"Price/Fruit"` udělením uživatelského přístupu k profilu `hlq.SUBSCRIBE.FRUIT` . Proveďte to pomocí následujících příkazů RACF :

  ```
  RDEFINE MXTOPIC hlq.SUBSCRIBE.FRUIT UACC(NONE)
  PERMIT hlq.SUBSCRIBE.FRUIT CLASS(MXTOPIC) ID(USER1) ACCESS(ALTER)
  ```

- Ostatní platformy:

  Udělte přístup k USER1 pro přihlášení k odběru tématu `"Price/Fruit"` udělením uživatelského přístupu k objektu FRUIT . Proveďte to pomocí příkazu autorizace pro platformu:

  ALW **Systémy AIX, Linux, and Windows**

  ```
  setmqaut -t topic -n FRUIT -p USER1 +sub
  ```

  IBM i **IBM i**

  ```
  GRTMQAUT OBJ(FRUIT) OBJTYPE(*TOPIC) USER(USER1) AUT(*SUB)
  ```

Výsledky

Když se USER1 pokusí přihlásit k odběru tématu `"Price/Fruit"` , výsledek je úspěšný.

Když se USER2 pokusí přihlásit k odběru tématu `"Price/Fruit"` , výsledkem je selhání se zprávou `MQRC_NOT_AUTHORIZED` , spolu s:

- z/OS V systému z/OSse na konzole zobrazují následující zprávy, které zobrazují úplnou cestu zabezpečení prostřednictvím stromu témat, o který jste se pokusili:

  ```
  ICH408I USER(USER2   ) ...
  ```

```
  hlq.SUBSCRIBE.FRUIT ...

ICH408I USER(USER2   ) ...
  hlq.SUBSCRIBE.SYSTEM.BASE.TOPIC ...
```

- ALW Na jiných platformách se jedná o následující událost autorizace:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit"
```

- IBM i V systému IBMi se jedná o následující událost autorizace:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit"
```

Všimněte si, že toto je ukázka toho, co vidíte; ne všechna pole.

Udělit uživateli přístup k odběru tématu hlouběji v rámci stromu

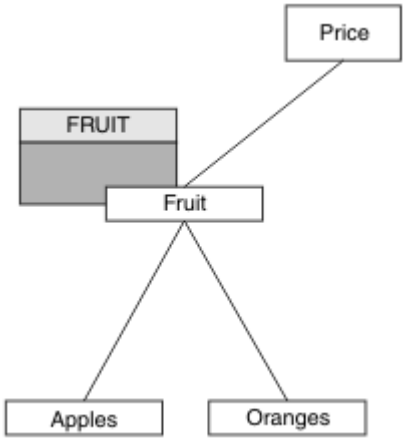
Toto téma je druhé v seznamu úloh, které vám sdělí, jak udělit přístup k tématům více než jednomu uživateli.

Než začnete

Toto téma používá nastavení popsané v části “Udělit uživateli přístup k odběru tématu” na stránce 508.

Informace o této úloze

Pokud bod ve stromu témat, ve kterém aplikace provádí odběr, není reprezentován objektem administrativního tématu, přesuňte strom nahoru, dokud nebude nalezen nejbližší nadřízený objekt administrativního tématu. Profil zabezpečení je kontrolován na základě názvu daného objektu tématu.



Obrázek 24. Příklad udělení přístupu k tématu v rámci stromu témat

Tabulka 90. Požadavky na přístup například k tématům a objektům témat

Téma	Je vyžadován přístup k odběru	Objekt tématu
Cena	Žádný uživatel	Není

Tabulka 90. Požadavky na přístup například k tématům a objektům témat (pokračování)		
Téma	**Je vyžadován přístup k odběru**	**Objekt tématu**
Cena/ovoce	USER1	OVOCE
Cena/ovoce/jablka	USER1	
Cena/ovoce/pomeranče	USER1	

V předchozí úloze USER1 byl udělen přístup k odběru tématu `"Price/Fruit"` udělením přístupu k profilu `hlq.SUBSCRIBE.FRUIT` on z/OS a přístupem k odběru profilu FRUIT na jiných platformách. Tento jediný profil také uděluje přístup USER1 k odběru pro `"Price/Fruit/Apples"`, `"Price/Fruit/Oranges"` a `"Price/Fruit/#"`.

Když se USER1 pokusí přihlásit k odběru tématu `"Price/Fruit/Apples"` , výsledek je úspěšný.

Když se USER2 pokusí přihlásit k odběru tématu `"Price/Fruit/Apples"` , výsledkem je selhání se zprávou `MQRC_NOT_AUTHORIZED` , spolu s:

- V systému z/OSse na konzole zobrazují následující zprávy, které zobrazují úplnou cestu zabezpečení prostřednictvím stromu témat, o který jste se pokusili:

```
ICH408I USER(USER2   ) ...
  hlq.SUBSCRIBE.FRUIT ...

ICH408I USER(USER2   ) ...
  hlq.SUBSCRIBE.SYSTEM.BASE.TOPIC ...
```

- Na jiných platformách se jedná o následující událost autorizace:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit/Apples"
```

Všimněte si následujícího:

- Zprávy, které obdržíte v systému z/OS , jsou stejné jako zprávy přijaté v předchozí úloze, protože přístup řídí stejné objekty tématu a profily.
- Zpráva události, kterou obdržíte na jiných platformách, je podobná zprávě přijaté v předchozí úloze, ale skutečný řetězec tématu se liší.

Udělit jinému uživateli přístup k odběru pouze tématu hlouběji v rámci stromu

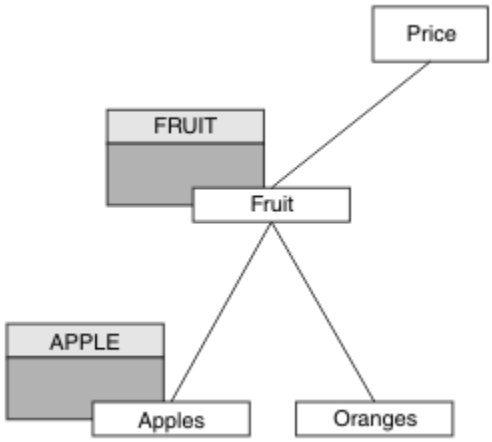
Toto téma je třetí v seznamu úloh, který uvádí, jak udělit přístup k odběru témat více než jedním uživatelem.

Než začnete

Toto téma používá nastavení popsané v části “Udělit uživateli přístup k odběru tématu hlouběji v rámci stromu” na stránce 510.

Informace o této úloze

V předchozí úloze USER2 byl odepřen přístup k tématu `"Price/Fruit/Apples"`. Toto téma vám řekne, jak udělit přístup k tomuto tématu, ale ne k žádným jiným tématům.



Obrázek 25. Udělení přístupu ke specifickým tématům v rámci stromu témat

Tabulka 91. Požadavky na přístup například k tématům a objektům témat

Téma	Je vyžadován přístup k odběru	Objekt tématu
Cena	Žádný uživatel	Není
Cena/ovoce	USER1	OVOCE
Cena/ovoce/jablka	USER1 a USER2	Jablko
Cena/ovoce/pomeranče	USER1	

Definujte nový objekt tématu následujícím způsobem:

Postup

1. Zadejte příkaz MQSC `DEF TOPIC(APPLE) TOPICSTR('Price/Fruit/Apples')`.
2. Udělte přístup následujícím způsobem:

- z/OS **z/OS** :

  V předchozí úloze USER1 byl udělen přístup k odběru tématu `"Price/Fruit/Apples"` udělením uživatelského přístupu k profilu `hlq.SUBSCRIBE.FRUIT` .

  Tento jediný profil také udělil USER1 přístup k odběru produktu `"Price/Fruit/Oranges"` `"Price/Fruit/#"` a tento přístup zůstává i s přidáním nového objektu tématu a s profily, které jsou k němu přidruženy.

  Udělte přístup k USER2 pro přihlášení k odběru tématu `"Price/Fruit/Apples"` udělením uživatelského přístupu k profilu `hlq.SUBSCRIBE.APPLE` . Proveďte to pomocí následujících příkazů RACF :

  ```
  RDEFINE MXTOPIC hlq.SUBSCRIBE.APPLE UACC(NONE)
  PERMIT hlq.SUBSCRIBE.FRUIT APPLE(MXTOPIC) ID(USER2) ACCESS(ALTER)
  ```

- Ostatní platformy:

  V předchozí úloze USER1 byl udělen přístup k odběru tématu `"Price/Fruit/Apples"` udělením přístupu uživatele k odběru profilu `FRUIT` .

Tento jediný profil také udělil USER1 přístup pro přihlášení k odběru `"Price/Fruit/Oranges"` a `"Price/Fruit/#"`a tento přístup zůstává i po přidání nového objektu tématu a profilů, které jsou k němu přidruženy.

Udělte přístup k USER2 pro přihlášení k odběru tématu `"Price/Fruit/Apples"` udělením přístupu uživatele k odběru profilu `APPLE` . Proveďte to pomocí příkazu autorizace pro platformu:

ALW **Systémy AIX, Linux, and Windows**

```
setmqaut -t topic -n APPLE -p USER2 +sub
```

IBM i **IBM i**

```
GRTMQAUT OBJ(APPLE) OBJTYPE(*TOPIC) USER(USER2) AUT(*SUB)
```

Výsledky

V systému z/OS, když se produkt USER1 pokusí přihlásit k odběru tématu `"Price/Fruit/Apples"` , první kontrola zabezpečení profilu `hlq.SUBSCRIBE.APPLE` se nezdaří, ale při přesunu stromu umožní profil `hlq.SUBSCRIBE.FRUIT` přihlásit se k odběru uživatele USER1 , takže se odběr úspěšně provede a do volání MQSUB se neodešle žádný návratový kód. Pro první kontrolu se však vygeneruje zpráva RACF `ICH` :

```
ICH408I USER(USER1   ) ...
  hlq.SUBSCRIBE.APPLE ...
```

Když se USER2 pokusí přihlásit k odběru tématu `"Price/Fruit/Apples"` , výsledek je úspěšný, protože kontrola zabezpečení projde prvním profilem.

Když se USER2 pokusí přihlásit k odběru tématu `"Price/Fruit/Oranges"` , výsledkem je selhání se zprávou `MQRC_NOT_AUTHORIZED` , spolu s:

- z/OS V systému z/OSse na konzole zobrazují následující zprávy, které zobrazují úplnou cestu zabezpečení prostřednictvím stromu témat, o který jste se pokusili:

  ```
  ICH408I USER(USER2   ) ...
    hlq.SUBSCRIBE.FRUIT ...

  ICH408I USER(USER2   ) ...
    hlq.SUBSCRIBE.SYSTEM.BASE.TOPIC ...
  ```

- ALW Na platformách AIX, Linux, and Windows se jedná o následující událost autorizace:

  ```
  MQRC_NOT_AUTHORIZED
  ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
  UserIdentifier        USER2
  AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
  TopicString           "Price/Fruit/Oranges"
  ```

- IBM i V systému IBMi se jedná o následující událost autorizace:

  ```
  MQRC_NOT_AUTHORIZED
  ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
  UserIdentifier        USER2
  AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
  TopicString           "Price/Fruit/Oranges"
  ```

Nevýhodou tohoto nastavení je, že v systému z/OSobdržíte na konzole další zprávy `ICH` . Tomu se můžete vyhnout, pokud zabezpečíte strom témat jiným způsobem.

Změňte řízení přístupu, abyste se vyhnuli dalším zprávám

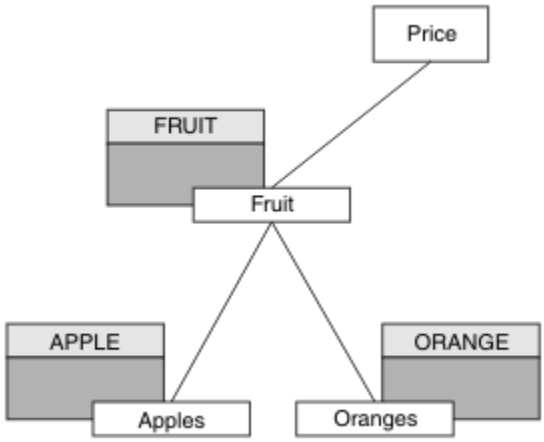
Toto téma je čtvrté v seznamu úloh, které vám říkají, jak udělit přístup k odběru témat více než jedním uživatelem a jak se vyhnout dalším zprávám RACF ICH408I na systému z/OS.

Než začnete

Toto téma rozšiřuje nastavení popsané v části “Udělit jinému uživateli přístup k odběru pouze tématu hlouběji v rámci stromu” na stránce 511 , abyste se vyhnuli dalším chybovým zprávám.

Informace o této úloze

Toto téma uvádí, jak udělit přístup k tématům hlouběji ve stromu a jak odebrat přístup k tématu níže ve stromu, když jej žádný uživatel nepožaduje.



Obrázek 26. Příklad udělení řízení přístupu, abyste se vyhnuli dalším zprávám.

Definujte nový objekt tématu následujícím způsobem:

Postup

1. Zadejte příkaz MQSC `DEF TOPIC(ORANGE) TOPICSTR('Price/Fruit/Oranges')`.
2. Udělte přístup následujícím způsobem:

   - z/OS **z/OS** :

     Definujte nový profil a přidejte k němu přístup a k existujícím profilům. Proveďte to pomocí následujících příkazů RACF :

     ```
     RDEFINE MXTOPIC hlq.SUBSCRIBE.ORANGE UACC(NONE)
     PERMIT hlq.SUBSCRIBE.ORANGE CLASS(MXTOPIC) ID(USER1) ACCESS(ALTER)
     PERMIT hlq.SUBSCRIBE.APPLE CLASS(MXTOPIC) ID(USER1) ACCESS(ALTER)
     ```

   - Ostatní platformy:

     Nastavte ekvivalentní přístup pomocí příkazů autorizace pro platformu:

     ALW **Systémy AIX, Linux, and Windows**

     ```
     setmqaut -t topic -n ORANGE -p USER1 +sub
     setmqaut -t topic -n APPLE -p USER1 +sub
     ```

IBM i

```
GRTMQAUT OBJ(ORANGE) OBJTYPE(*TOPIC) USER(USER1) AUT(*SUB)
GRTMQAUT OBJ(APPLE) OBJTYPE(*TOPIC) USER(USER1) AUT(*SUB)
```

Výsledky

V systému z/OS, když se produkt USER1 pokusí přihlásit k odběru tématu `"Price/Fruit/Apples"` , první kontrola zabezpečení v profilu `hlq.SUBSCRIBE.APPLE` uspěje.

Podobně, když se USER2 pokusí přihlásit k odběru tématu `"Price/Fruit/Apples"` , výsledek je úspěšný, protože kontrola zabezpečení předá první profil.

Když se USER2 pokusí přihlásit k odběru tématu `"Price/Fruit/Oranges"` , výsledkem je selhání se zprávou `MQRC_NOT_AUTHORIZED` , spolu s:

- z/OS V systému z/OSse na konzole zobrazují následující zprávy, které zobrazují úplnou cestu zabezpečení prostřednictvím stromu témat, o který jste se pokusili:

```
ICH408I USER(USER2   ) ...
  hlq.SUBSCRIBE.ORANGE ...

ICH408I USER(USER2   ) ...
  hlq.SUBSCRIBE.FRUIT ...

ICH408I USER(USER2   ) ...
  hlq.SUBSCRIBE.SYSTEM.BASE.TOPIC ...
```

- ALW Na jiných platformách se jedná o následující událost autorizace:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      ORANGE, FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit/Oranges"
```

- IBM i V systému IBMi se jedná o následující událost autorizace:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      ORANGE, FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit/Oranges"
```

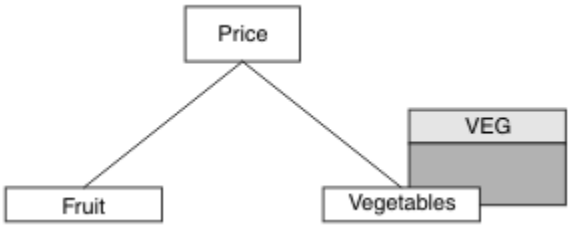
Udělit uživateli přístup pro publikování v tématu

Toto téma je první v seznamu úloh, které vám sdělí, jak udělit přístup pro publikování témat více než jedním uživatelem.

Informace o této úloze

Tato úloha předpokládá, že na pravé straně stromu témat neexistují žádné objekty administrativního tématu, ani nebyly definovány žádné profily pro publikování. Předpokládá se, že vydavatelé používají pouze řetězec tématu.

Aplikace může publikovat do tématu poskytnutím objektu tématu, řetězce tématu nebo kombinace obojího. Bez ohledu na to, jakým způsobem aplikace vybere, je výsledkem publikování v určitém bodě stromu témat. Pokud je tento bod ve stromu témat reprezentován objektem administrativního tématu, zkontroluje se profil zabezpečení na základě názvu tohoto objektu tématu. Příklad:



Obrázek 27. Udělení přístupu pro publikování k tématu

Tabulka 92. Příklad požadavků na přístup k publikování		
Téma	**Je vyžadován přístup pro publikování**	**Objekt tématu**
Cena	Žádný uživatel	Není
Cena/zelenina	USER1	VEG

Definujte nový objekt tématu následujícím způsobem:

Postup

1. Zadejte příkaz MQSC `DEF TOPIC(VEG) TOPICSTR('Price/Vegetables')`.
2. Udělte přístup následujícím způsobem:

- z/OS **z/OS** :

  Udělte přístup k USER1 pro publikování do tématu `"Price/Vegetables"` udělením uživatelského přístupu k profilu `hlq.PUBLISH.VEG` . Proveďte to pomocí následujících příkazů RACF :

  ```
  RDEFINE MXTOPIC hlq.PUBLISH.VEG UACC(NONE)
  PERMIT hlq.PUBLISH.VEG CLASS(MXTOPIC) ID(USER1) ACCESS(UPDATE)
  ```

- Ostatní platformy:

  Udělte přístup k USER1 pro publikování do tématu `"Price/Vegetables"` udělením uživatelského přístupu k profilu VEG . Proveďte to pomocí příkazu autorizace pro platformu:

  ALW **Systémy AIX, Linux, and Windows**

  ```
  setmqaut -t topic -n VEG -p USER1 +pub
  ```

  IBM i **IBM i**

  ```
  GRTMQAUT OBJ(VEG) OBJTYPE(*TOPIC) USER(USER1) AUT(*PUB)
  ```

Výsledky

Když se USER1 pokusí publikovat do tématu `"Price/Vegetables"` , výsledek je úspěšný; to znamená, že volání MQOPEN je úspěšné.

Když se USER2 pokusí publikovat do tématu `"Price/Vegetables"` volání MQOPEN selže se zprávou `MQRC_NOT_AUTHORIZED` , spolu s:

- z/OS V systému z/OSse na konzole zobrazují následující zprávy, které zobrazují úplnou cestu zabezpečení prostřednictvím stromu témat, o který jste se pokusili:

```
ICH408I USER(USER2   ) ...
  hlq.PUBLISH.VEG ...

ICH408I USER(USER2   ) ...
  hlq.PUBLISH.SYSTEM.BASE.TOPIC ...
```

- ALW Na jiných platformách se jedná o následující událost autorizace:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_OPEN_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      VEG, SYSTEM.BASE.TOPIC
TopicString           "Price/Vegetables"
```

- IBM i V systému IBMi se jedná o následující událost autorizace:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_OPEN_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      VEG, SYSTEM.BASE.TOPIC
TopicString           "Price/Vegetables"
```

Všimněte si, že toto je ukázka toho, co vidíte; ne všechna pole.

Udělit uživateli přístup k publikování tématu hlouběji v rámci stromu.

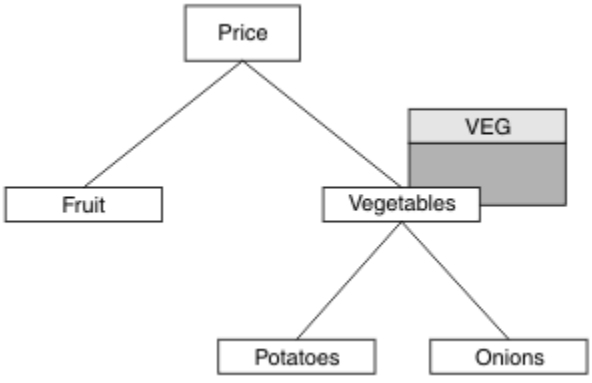
Toto téma je druhé v seznamu úloh, které vám sdělí, jak udělit přístup k tématům pro publikování více než jedním uživatelem.

Než začnete

Toto téma používá nastavení popsané v části “Udělit uživateli přístup pro publikování v tématu” na stránce 515.

Informace o této úloze

Pokud bod ve stromu témat, ve kterém je aplikace publikována, není reprezentován objektem administrativního tématu, přesuňte strom nahoru, dokud nebude nalezen nejbližší nadřízený objekt administrativního tématu. Profil zabezpečení je kontrolován na základě názvu daného objektu tématu.



Obrázek 28. Udělení přístupu pro publikování k tématu v rámci stromu témat

Tabulka 93. Příklad požadavků na přístup k publikování

Téma	Je vyžadován přístup k odběru	Objekt tématu
Cena	Žádný uživatel	Není
Cena/zelenina	USER1	VEG
Cena/zelenina/brambory	USER1	
Cena/zelenina/cibule	USER1	

V předchozí úloze USER1 byl udělen přístup k tématu publikování `"Price/Vegetables/Potatoes"` udělením přístupu k profilu `hlq.PUBLISH.VEG` v systému z/OS nebo publikováním přístupu k profilu `VEG` na jiných platformách. Tento jediný profil také uděluje USER1 přístup k publikování na adrese `"Price/Vegetables/Onions"`.

Když se USER1 pokusí publikovat v tématu `"Price/Vegetables/Potatoes"` , výsledek je úspěšný; to znamená, že volání MQOPEN je úspěšné.

Při USER2 pokusech o přihlášení k odběru tématu `"Price/Vegetables/Potatoes"` dojde k selhání; to znamená, že volání MQOPEN selže se zprávou `MQRC_NOT_AUTHORIZED` spolu s:

- V systému z/OSse na konzole zobrazují následující zprávy, které zobrazují úplnou cestu zabezpečení prostřednictvím stromu témat, o který jste se pokusili:

```
ICH408I USER(USER2   ) ...
  hlq.PUBLISH.VEG ...

ICH408I USER(USER2   ) ...
  hlq.PUBLISH.SYSTEM.BASE.TOPIC ...
```

- Na jiných platformách se jedná o následující událost autorizace:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_OPEN_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      VEG, SYSTEM.BASE.TOPIC
TopicString           "Price/Vegetables/Potatoes"
```

Všimněte si následujícího:

- Zprávy, které obdržíte v systému z/OS , jsou stejné jako zprávy přijaté v předchozí úloze, protože přístup řídí stejné objekty tématu a profily.
- Zpráva události, kterou obdržíte na jiných platformách, je podobná zprávě přijaté v předchozí úloze, ale skutečný řetězec tématu se liší.

Udělit přístup pro publikování a odběr

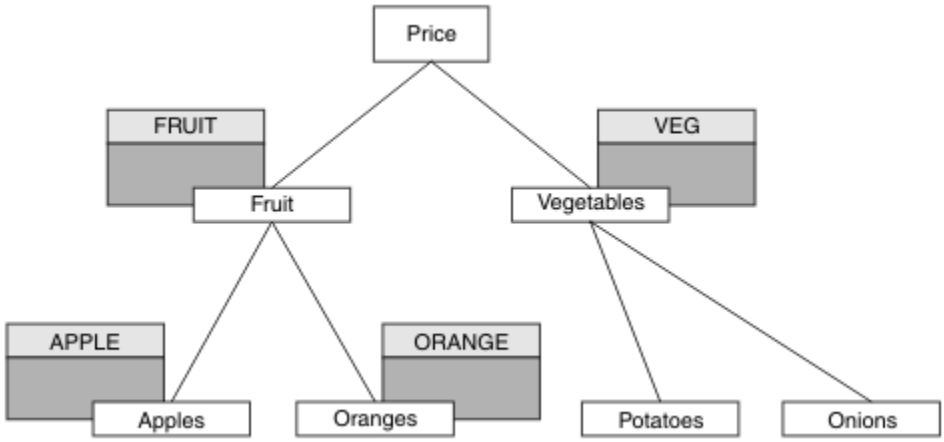
Toto téma je poslední v seznamu úloh, který uvádí, jak udělit přístup k publikování a přihlášení k odběru témat více než jedním uživatelem.

Než začnete

Toto téma používá nastavení popsané v části “Udělit uživateli přístup k publikování tématu hlouběji v rámci stromu.” na stránce 517.

Informace o této úloze

V předchozí úloze USER1 byl udělen přístup k odběru tématu `"Price/Fruit"`. Toto téma uvádí, jak udělit uživateli přístup k publikování tohoto tématu.



Obrázek 29. Udělení přístupu pro publikování a odběr

Tabulka 94. Příklad požadavků na publikování a přihlášení k odběru přístupu

Téma	Je vyžadován přístup k odběru	Je vyžadován přístup pro publikování	Objekt tématu
Cena	Žádný uživatel	Žádný uživatel	Není
Cena/ovoce	USER1	USER1	OVOCE
Cena/ovoce/jablka	USER1 a USER2		Jablko
Cena/ovoce/pomeranče	USER1		ORANŽOVÁ

Postup

Udělte přístup následujícím způsobem:

- z/OS **z/OS** :

  V dřívější úloze USER1 byl udělen přístup k odběru tématu `"Price/Fruit"` udělením uživatelského přístupu k profilu `hlq.SUBSCRIBE.FRUIT` .

  Chcete-li publikovat v tématu `"Price/Fruit"` , udělte přístup k USER1 profilu `hlq.PUBLISH.FRUIT` . Proveďte to pomocí následujících příkazů RACF :

  ```
  RDEFINE MXTOPIC hlq.PUBLISH.FRUIT UACC(NONE)
  PERMIT hlq.PUBLISH.FRUIT CLASS(MXTOPIC) ID(USER1) ACCESS(ALTER)
  ```

- Ostatní platformy:

  Udělte přístup k USER1 pro publikování do tématu `"Price/Fruit"` udělením uživatelského publikačního přístupu k profilu FRUIT . Proveďte to pomocí příkazu autorizace pro platformu:

  ALW **Systémy AIX, Linux, and Windows**

  ```
  setmqaut -t topic -n FRUIT -p USER1 +pub
  ```

IBM i

```
GRTMQAUT OBJ(FRUIT) OBJTYPE(*TOPIC) USER(USER1) AUT(*PUB)
```

Výsledky

V systému z/OSplatí, že když se produkt USER1 pokusí publikovat do tématu `"Price/Fruit"` , kontrola zabezpečení volání MQOPEN proběhne úspěšně.

Když se USER2 pokusí publikovat v tématu `"Price/Fruit"` , výsledkem je selhání se zprávou `MQRC_NOT_AUTHORIZED` , spolu s:

- V systému z/OSse na konzole zobrazují následující zprávy, které zobrazují úplnou cestu zabezpečení prostřednictvím stromu témat, o který jste se pokusili:

```
ICH408I USER(USER2   ) ...
  hlq.PUBLISH.FRUIT ...

ICH408I USER(USER2   ) ...
  hlq.PUBLISH.SYSTEM.BASE.TOPIC ...
```

- Na platformách AIX, Linux, and Windows se jedná o následující událost autorizace:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_OPEN_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit"
```

- V systému IBM ise jedná o následující událost autorizace:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_OPEN_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit"
```

Po provedení úplné sady těchto úloh získá produkt USER1 a USER2 následující přístupová oprávnění pro publikování a odběr uvedených témat:

Tabulka 95. Úplný seznam přístupových oprávnění vyplývajících z příkladů zabezpečení

Téma	Je vyžadován přístup k odběru	Je vyžadován přístup pro publikování	Objekt tématu
Cena	Žádný uživatel	Žádný uživatel	Není
Cena/ovoce	USER1	USER1	OVOCE
Cena/ovoce/jablka	USER1 a USER2		Jablko
Cena/ovoce/pomeranče	USER1		ORANŽOVÁ
Cena/zelenina		USER1	VEG

Tabulka 95. Úplný seznam přístupových oprávnění vyplývajících z příkladů zabezpečení (pokračování)			
Téma	**Je vyžadován přístup k odběru**	**Je vyžadován přístup pro publikování**	**Objekt tématu**
Cena/ zelenina/ brambory			
Cena/ zelenina/ cibule			

Pokud máte různé požadavky na zabezpečený přístup na různých úrovních v rámci stromu témat, pečlivé plánování zajistí, že v protokolu konzoly z/OS neobdržíte vnější varování zabezpečení. Nastavením zabezpečení na správné úrovni v rámci stromu se vyhnete zavádějícím zprávám zabezpečení.

Zabezpečení odběru

MQSO_ALTERNATE_USER_AUTHORITY

Pole AlternateUserId obsahuje identifikátor uživatele, který se má použít k ověření tohoto volání MQSUB. Volání může být úspěšné pouze v případě, že je toto ID AlternateUserautorizováno pro přihlášení k odběru tématu se zadanými volbami přístupu, bez ohledu na to, zda je k tomu autorizován identifikátor uživatele, pod kterým je aplikace spuštěna.

MQSO_SET_IDENTITY_CONTEXT

Odběr má používat data identity tokenu evidence a aplikace dodaná v polích PubAccountingToken a PubApplIdentityData .

Je-li zadána tato volba, provede se stejná kontrola autorizace, jako kdyby k cílové frontě bylo přistupováno pomocí volání MQOPEN s volbou MQOO_SET_IDENTITY_CONTEXT, s výjimkou případu, kdy je použita také volba MQSO_MANAGED, v němž neexistuje žádná kontrola autorizace v cílové frontě.

Není-li tato volba určena, jsou k publikacím odesílaným tomuto odběrateli přidruženy výchozí informace o kontextu, a to následujícím způsobem:

Tabulka 96. Výchozí informace o kontextu publikování	
Pole v deskriptoru MQMD	**Použitá hodnota**
UserIdentifier	ID uživatele přidružené k odběru (viz pole SUBUSER na obrazovce DISPLAY SBSTATUS) v době publikování.
AccountingToken	Určuje se z prostředí, je-li to možné; jinak nastavte na hodnotu MQACT_NONE.
ApplIdentityData	Nastavte na mezery.

Tato volba je platná pouze pro příkazy MQSO_CREATE a MQSO_ALTER. V případě použití s poli MQSO_RESUME jsou pole PubAccountingToken a PubApplIdentityData ignorována, takže tato volba nemá žádný vliv.

Je-li odběr změněn bez použití této volby, kde dříve předplatil informace o kontextu identity, budou pro změněný odběr vygenerovány výchozí informace o kontextu.

Pokud je odběr, který umožňuje použití různých ID uživatelů s volbou MQSO_ANY_USERID, obnoven jiným ID uživatele, vygeneruje se výchozí kontext identity pro nové ID uživatele, které nyní vlastní odběr, a všechna následná publikování budou doručena s novým kontextem identity.

AlternateSecurityId

Jedná se o identifikátor zabezpečení, který je předán s ID AlternateUserautorizační službě, aby bylo možné provést odpovídající kontroly autorizace. AlternateSecurityId se používá pouze v případě, že je uvedeno MQSO_ALTERNATE_USER_AUTHORITY a pole AlternateUserId není zcela prázdné až do prvního znaku null nebo konce pole.

Volba odběru MQSO_ANY_USERID

Je-li zadána hodnota MQSO_ANY_USERID, není identita odběratele omezena na jediné ID uživatele. To umožňuje každému uživateli změnit nebo obnovit odběr, pokud má odpovídající oprávnění. Odběr může mít v daném okamžiku pouze jeden uživatel. Pokus o obnovení použití odběru, který je aktuálně používán jinou aplikací, způsobí selhání volání MQRC_SUBSCRIPTION_IN_USE.

Chcete-li přidat tuto volbu k existujícímu odběru, musí volání MQSUB (pomocí příkazu MQSO_ALTER) pocházet ze stejného ID uživatele jako původní odběr.

Pokud volání MQSUB odkazuje na existující odběr se sadou MQSO_ANY_USERID a ID uživatele se liší od původního odběru, volání bude úspěšné pouze v případě, že nové ID uživatele má oprávnění k odběru tématu. Po úspěšném dokončení jsou budoucí publikování pro tohoto odběratele vložena do fronty odběratele s novým ID uživatele nastaveným v publikování.

MQSO_FIXED_USERID

Je-li zadána hodnota MQSO_FIXED_USERID, může být odběr změněn nebo obnoven pouze jedním vlastnícím ID uživatele. Toto ID uživatele je posledním ID uživatele, které změnilo odběr, který nastavil tuto volbu, a odebrali tak volbu MQSO_ANY_USERID, nebo pokud nedošlo ke změně, jedná se o ID uživatele, který vytvořil odběr.

Pokud příkaz MQSUB odkazuje na existující odběr se sadou MQSO_ANY_USERID a změní odběr (pomocí příkazu MQSO_ALTER) tak, aby používal volbu MQSO_FIXED_USERID, bude ID uživatele odběru nyní opraveno na toto nové ID uživatele. Volání je úspěšné pouze v případě, že nové ID uživatele má oprávnění přihlásit se k odběru tématu.

Pokud ID uživatele jiné, než které bylo zaznamenáno jako vlastník odběrů trys pro obnovení nebo změnu odběru MQSO_FIXED_USERID, volání se nezdaří s MQRC_IDENTITY_MISMATCH. ID vlastnícího uživatele odběru lze zobrazit pomocí příkazu DISPLAY SBSTATUS.

Není-li zadána hodnota MQSO_ANY_USERID ani MQSO_FIXED_USERID, bude použita výchozí hodnota MQSO_FIXED_USERID.

Zabezpečení publikování/odběru mezi správci front

Interní zprávy publikování/odběru, například proxy odběry a publikování, jsou vloženy do systémových front publikování/odběru s použitím běžných pravidel zabezpečení kanálu. Informace a diagramy v tomto tématu zvýrazňují různé procesy a ID uživatelů, které se podílejí na doručování těchto zpráv.

Lokální řízení přístupu

Přístup k tématům pro publikování a odběry se řídí lokálními definicemi zabezpečení a pravidly, která jsou popsána v tématu Zabezpečení publikování/odběru. V systému z/OSnení pro zavedení řízení přístupu vyžadován žádný lokální objekt tématu. Pro řízení přístupu na jiných platformách není vyžadováno žádné lokální téma. Administrátoři se mohou rozhodnout použít řízení přístupu na klastrované objekty tématu bez ohledu na to, zda v klastru dosud existují.

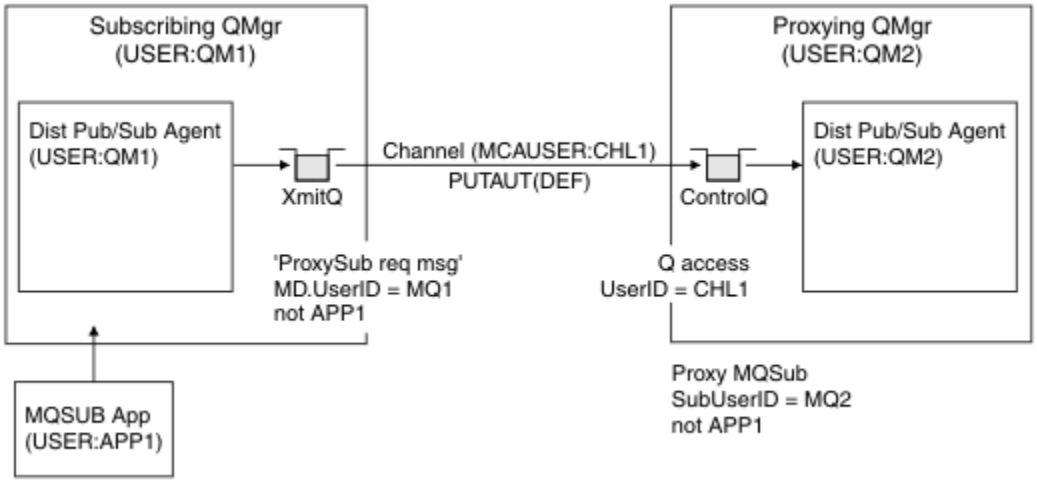
Administrátoři systému jsou zodpovědní za řízení přístupu na svém lokálním systému. Musí důvěřovat administrátorům ostatních členů hierarchie nebo kolektivů klastru, aby byli zodpovědní za své zásady

řízení přístupu. Vzhledem k tomu, že řízení přístupu je definováno pro každý samostatný stroj, je pravděpodobné, že bude zatěžující, pokud je zapotřebí jemná kontrola úrovně. Nemusí být nutné vynutit žádné řízení přístupu, nebo může být řízení přístupu definováno na objektech vysoké úrovně ve stromu témat. Řízení přístupu na jemné úrovni lze definovat pro každé pododdělení oboru názvů témat.

Vytvoření proxy odběru

Důvěryhodnost organizace pro připojení jejího správce front ke správci front je potvrzena běžnými prostředky ověřování kanálu. Pokud má tato důvěryhodná organizace také povoleno provádět distribuované publikování/odběr, provede se kontrola oprávnění. Kontrola se provede, když kanál vloží zprávu do distribuované fronty publikování/odběru. Například, pokud je zpráva vložena do fronty SYSTEM.INTER.QMGR.CONTROL . ID uživatele pro kontrolu oprávnění fronty závisí na hodnotách PUTAUT přijímajícího kanálu. Například ID uživatele kanálu MCAUSER, kontext zprávy, v závislosti na hodnotě a platformě. Další informace o zabezpečení kanálu naleznete v tématu Zabezpečení kanálu.

Proxy odběry jsou prováděny s ID uživatele distribuovaného agenta publikování/odběru ve vzdáleném správci front. Například QM2 v adresáři Obrázek 30 na stránce 523. Uživateli je pak snadno udělen přístup k lokálním profilům objektů tématu, protože toto ID uživatele je definováno v systému, a proto nedochází ke konfliktům v doméně.



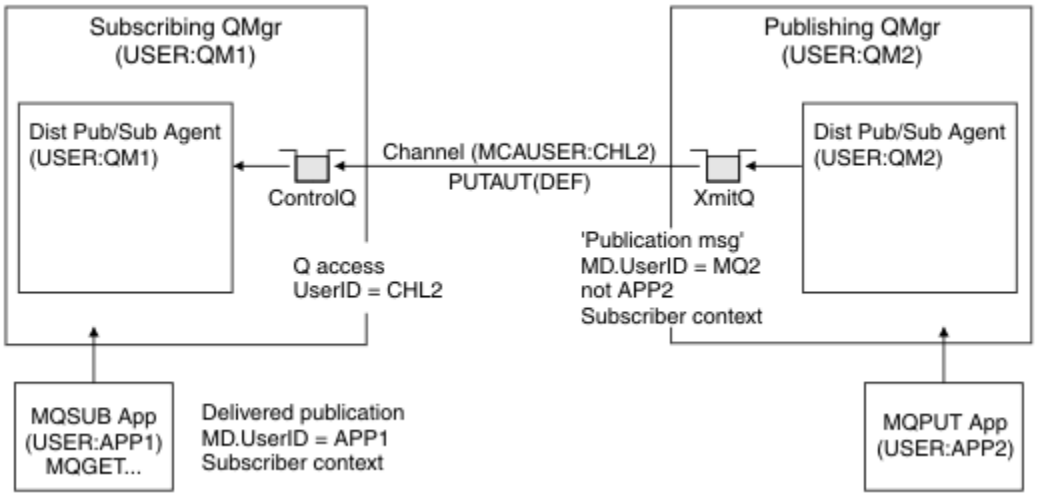
Obrázek 30. zabezpečení proxy odběru, vytvoření odběru

Odesílání zpět vzdálených publikací

Při vytvoření publikování ve správci front publikování je vytvořena kopie publikování pro všechny proxy odběry. Kontext zkopírovaného publikování obsahuje kontext ID uživatele, který provedl odběr; QM2 v souboru Obrázek 31 na stránce 524. Proxy odběr je vytvořen s cílovou frontou, která je vzdálenou frontou, takže zpráva publikování je interpretována jako přenosová fronta.

Důvěryhodnost organizace pro připojení správce front QM2k jinému správci front QM1je potvrzena běžnými prostředky ověřování kanálu. Pokud je pak této důvěryhodné organizaci povoleno provádět distribuované publikování/odběr, provede se kontrola oprávnění, když kanál vloží zprávu publikování do fronty publikování distribuovaného publikování/odběru SYSTEM.INTER.QMGR.PUBS. ID uživatele pro kontrolu oprávnění fronty závisí na hodnotě PUTAUT přijímacího kanálu (například ID uživatele kanálu, MCAUSER, kontext zprávy a další, v závislosti na hodnotě a platformě). Další informace o zabezpečení kanálu naleznete v tématu Zabezpečení kanálu.

Když zpráva publikování dosáhne správce front odběru, provede se další operace MQPUT do tématu pod autoritou tohoto správce front a kontext se zprávou je nahrazen kontextem každého z lokálních odběratelů, jak jsou jednotlivým zprávám dány.



Obrázek 31. Zabezpečení proxy odběru, předávání publikací

V systému, v němž bylo zvažováno málo z hlediska zabezpečení, jsou distribuované procesy publikování/odběru pravděpodobně spuštěny pod ID uživatele ve skupině `mqm` , parametr `MCAUSER` na kanálu je prázdný (výchozí nastavení) a zprávy jsou podle potřeby doručovány do různých systémových front. Nezabezpečený systém usnadňuje nastavení důkazu o koncepci pro demonstraci distribuovaného publikování/odběru.

V systému, kde je zabezpečení vážněji zvažováno, podléhají tyto interní zprávy stejným bezpečnostním kontrolám jako všechny zprávy, které jdou přes kanál.

Je-li kanál nastaven s neprázdnou hodnotou `MCAUSER` a hodnotou `PUTAUT` , která určuje, že musí být zaškrtnuto políčko `MCAUSER` , musí být danému uživateli `MCAUSER` udělen přístup k frontám `SYSTEM.INTER.QMGR.*` . Pokud existuje více různých vzdálených správců front s kanály spuštěnými pod různými ID `MCAUSER` , musí být všem těmto ID uživatelů udělen přístup k frontám `SYSTEM.INTER.QMGR.*` . Kanály spuštěné pod různými ID `MCAUSER` se mohou vyskytovat například v případě, že je v jednom správci front konfigurováno více hierarchických připojení.

Je-li kanál nastaven s hodnotou `PUTAUT` určující, že je použit kontext zprávy, bude kontrolován přístup k frontám `SYSTEM.INTER.QMGR.*` na základě ID uživatele v interní zprávě. Vzhledem k tomu, že všechny tyto zprávy jsou vloženy s ID uživatele distribuovaného agenta publikování/odběru ze správce front, který odesílá interní zprávu, nebo publikační zprávu (viz Obrázek 31 na stránce 524), není příliš velká sada ID uživatelů pro udělení přístupu k různým systémovým frontám (jeden pro každého vzdáleného správce front), pokud chcete tímto způsobem nastavit distribuované zabezpečení publikování/odběru. Stále má všechny stejné problémy, které má zabezpečení kontextu kanálu vždy; problémy různých domén ID uživatele a skutečnost, že ID uživatele ve zprávě nemusí být definováno v přijímajícím systému. Nicméně, je to naprosto přijatelný způsob, jak spustit v případě potřeby.

z/OS Zabezpečení systémové fronty poskytuje seznam front a přístup, který je nezbytný k bezpečnému nastavení distribuovaného prostředí publikování/odběru. Pokud se nezdaří vložení interních zpráv nebo publikování v důsledku narušení zabezpečení, kanál zapíše zprávu do protokolu běžným způsobem a zprávy lze odeslat do fronty nedoručených zpráv v souladu s běžným zpracováním chyb kanálu.

Všechny systémy zpráv mezi správci front pro účely distribuovaného publikování/odběru jsou spouštěny s použitím normálního zabezpečení kanálu.

Informace o omezení publikování a proxy odběrů na úrovni tématu naleznete v tématu Zabezpečení publikování/odběru.

Použití výchozích ID uživatelů s hierarchií správce front

Máte-li hierarchii správců front spuštěných na různých platformách a používáte-li výchozí ID uživatelů, mějte na paměti, že tato výchozí ID uživatelů se mezi jednotlivými platformami liší a nemusí být na cílové

platformě známa. V důsledku toho správce front spuštěný na jedné platformě odmítne zprávy přijaté od správců front na jiných platformách s kódem příčiny MQRC_NOT_AUTHORIZED.

Chcete-li se vyhnout odmítnutí zpráv, je třeba do výchozích ID uživatelů používaných na jiných platformách přidat alespoň následující oprávnění:

- Oprávnění *PUT *GET na SYSTEM.BROKER. fronty
- *PUB *SUB oprávnění na SYSTEM.BROKER. Témata
- *ADMCRT *ADMDLT *ADMCHG oprávnění na SYSTEM.BROKER.CONTROL.QUEUE .

Výchozí ID uživatelů s hierarchií správců front jsou následující:

Platforma	Předvolené ID uživatele
Windows	mqm
Systémy AIX and Linux	mqm
IBM i	QMQM
z/OS	ID uživatele adresního prostoru inicializátoru kanálu

Vytvořte a udělte přístup k ID uživatele 'qmqm', pokud je hierarchicky připojen ke správci front v systému IBM i pro správce front na platformách z/OS, AIX, Linux, and Windows .

Pro správce front na platformách IBM i a z/OS vytvořte a udělte přístup k ID uživatele 'mqm', pokud je hierarchicky připojen ke správci front na systému AIX, Linux, and Windows .

Vytvořte a udělte uživateli přístup k ID uživatele adresního prostoru inicializátoru kanálu z/OS , pokud je hierarchicky připojen ke správci front v systému z/OS pro správce front v systému Multiplatforms.

ID uživatelů mohou rozlišovat malá a velká písmena. Původní správce front (je-li v systému Multiplatforms) vynutí, aby bylo jméno uživatele uvedeno velkými písmeny. Přijímající správce front (pokud je v systému AIX, Linux, and Windows) vynutí, aby ID uživatele bylo malé. Proto musí být všechna ID uživatelů vytvořená v systémech AIX and Linux vytvořena ve tvaru malých písmen. Pokud byla instalována uživatelská procedura pro zprávy, nevynucení ID uživatele na velká nebo malá písmena se neprovede. Je třeba dbát na to, abyste porozuměli tomu, jak uživatelská procedura zprávy zpracovává ID uživatele.

Chcete-li se vyhnout možným problémům s převodem ID uživatelů, postupujte takto:

- Na systémech AIX, Linux, and Windows se ujistěte, že jsou ID uživatelů uvedena malými písmeny.
- V systémech IBM i a z/OSse ujistěte, že ID uživatelů jsou zadána velkými písmeny.

Zabezpečení IBM MQ Console a REST API

Zabezpečení pro IBM MQ Console a REST API se konfiguruje úpravou konfigurace serveru mqweb v souboru mqwebuser.xml .

Informace o této úloze

Můžete sledovat akce uživatele a auditovat použití IBM MQ Console a REST API kontrolou souborů protokolu serveru mqweb.

Uživatele IBM MQ Console a REST API lze ověřit pomocí:

- Základní registr
- Registr LDAP
- Registr lokálního operačního systému
- SAF v systému z/OS
- Jakýkoli jiný typ registru podporovaný produktem WebSphere Liberty

Role mohou být přiřazeny uživatelům produktu IBM MQ Console a uživatelům produktu REST API k určení úrovně přístupu, které jsou uděleny objektům produktu IBM MQ . Chcete-li například provádět zasílání zpráv, musí být uživatelům přiřazena role `MQWebUser` . Další informace o dostupných rolích viz “Role na IBM MQ Console a REST API” na stránce 537.

Po přiřazení role uživateli existuje řada metod, které lze použít k ověření uživatele. Pomocí konzoly IBM MQ Consolese mohou uživatelé přihlásit pomocí jména uživatele a hesla, nebo mohou použít ověření pomocí certifikátu klienta. S produktem REST APImohou uživatelé používat základní ověřování HTTP , ověřování založené na tokenech nebo ověřování pomocí certifikátu klienta.

Postup

1. Definujte registr uživatelů pro ověření uživatelů a přiřaďte každému uživateli nebo skupině roli pro autorizaci uživatelů a skupin pro použití IBM MQ Console nebo REST API. Další informace naleznete zde: “Konfigurace uživatelů a rolí” na stránce 527
2. Zvolte, jak se uživatelé produktu IBM MQ Console ověřují na serveru mqweb. Nemusíte používat stejnou metodu pro všechny uživatele:
   - Umožnit uživatelům ověřit se pomocí ověření tokenu. V tomto případě uživatel zadá ID uživatele a heslo na přihlašovací obrazovce produktu IBM MQ Console . Je vygenerován token LTPA, který uživateli umožňuje zůstat přihlášený a autorizovaný po nastavenou dobu. Pro použití této volby ověřování není vyžadována žádná další konfigurace, můžete však volitelně konfigurovat dobu vypršení platnosti tokenu LTPA. Další informace naleznete v tématu Konfigurace intervalu vypršení platnosti tokenu LTPA.
   - Umožnit uživatelům ověřit se pomocí certifikátů klienta. V tomto případě uživatel nepoužívá ID uživatele nebo heslo pro přihlášení k serveru IBM MQ Console, ale místo toho používá certifikát klienta. Další informace viz téma “Použití ověření pomocí certifikátu klienta s REST API a IBM MQ Console” na stránce 542.
3. Zvolte, jak se uživatelé produktu REST API ověřují na serveru mqweb. Nemusíte používat stejnou metodu pro všechny uživatele:
   - Umožnit uživatelům ověření pomocí základního ověření HTTP . V tomto případě je jméno uživatele a heslo zakódováno, ale není šifrováno, a odesláno s každým požadavkem REST API pro ověření a autorizaci uživatele pro tento požadavek. Aby bylo toto ověření zabezpečené, musíte použít zabezpečené připojení. To znamená, že musíte použít HTTPS. Další informace viz téma “Použití základního ověření HTTP s REST API” na stránce 546.
   - Umožnit uživatelům ověřit se pomocí ověření tokenu. V tomto případě uživatel poskytne ID uživatele a heslo pro prostředek REST API `login` pomocí metody HTTP POST. Je vygenerován token LTPA, který uživateli umožňuje zůstat přihlášený a autorizovaný po nastavenou dobu. Další informace viz téma “Použití ověření založeného na tokenech s rozhraním REST API” na stránce 547.

     Aby bylo toto ověření zabezpečené, musíte použít zabezpečené připojení. To znamená, že musíte použít HTTPS. Pokud jste však povolili připojení HTTP , můžete povolit použití tokenu LTPA, který je vydán pro připojení HTTPS , pro připojení HTTP . Další informace viz Konfigurace tokenu LTPA.
   - Umožnit uživatelům ověřit se pomocí certifikátů klienta. V tomto případě uživatel nepoužívá ID uživatele nebo heslo pro přihlášení k serveru REST API, ale místo toho používá certifikát klienta. Další informace viz téma “Použití ověření pomocí certifikátu klienta s REST API a IBM MQ Console” na stránce 542.
4. Volitelné: Nakonfigurujte sdílení prostředků mezi zdroji pro REST API.

   Standardně webový prohlížeč nedovoluje skriptům, jako je JavaScript, vyvolat skript REST API , když není ze stejného původu jako skript REST API. To znamená, že požadavky na křížový původ nejsou povoleny. Můžete konfigurovat sdílení CORS (Cross Origin Resource Sharing), abyste povolili požadavky na křížový původ z určených adres URL. Další informace viz téma “Konfigurace CORS pro REST API” na stránce 549.
5. Volitelné: Nakonfigurujte ověření záhlaví hostitele pro IBM MQ Console a REST API.

Můžete nakonfigurovat ověření záhlaví hostitele a vytvořit seznam povolených názvů hostitelů a portů, abyste zajistili, že produkty IBM MQ Console a REST APIzpracují pouze požadavky, které obsahují specifická záhlaví hostitele. Další informace viz téma “Konfigurace ověření záhlaví hostitele pro IBM MQ Console a REST API” na stránce 550.

Konfigurace uživatelů a rolí

Chcete-li použít IBM MQ Console nebo REST API, uživatelé se musí ověřit vůči registru uživatelů definovanému na serveru mqweb.

Informace o této úloze

Ověření uživatelé musí být členem jedné ze skupin, které autorizují přístup ke schopnostem produktů IBM MQ Console a REST API. Standardně registr uživatelů neobsahuje žádné uživatele; ty je třeba přidat úpravou souboru `mqwebuser.xml` .

Když konfigurujete uživatele a skupiny, nejprve nakonfigurujete registr uživatelů, abyste ověřili uživatele a skupiny. Tento registr uživatelů je sdílen mezi IBM MQ Console a REST API. Při konfiguraci rolí pro uživatele a skupiny můžete řídit, zda mají uživatelé a skupiny přístup k serveru IBM MQ Console, REST APInebo k oběma.

Poté, co nakonfigurujete registr uživatelů, nakonfigurujete role pro uživatele a skupiny, aby jim udělily autorizaci. K dispozici je několik rolí, včetně rolí specifických pro použití REST API pro Managed File Transfer. Každá role uděluje jinou úroveň přístupu. Další informace viz téma “Role na IBM MQ Console a REST API” na stránce 537.

Na serveru mqweb je k dispozici řada ukázkových souborů XML, které zjednodušují konfiguraci uživatelů a skupin. Uživatelé, kteří jsou obeznámeni s konfigurací zabezpečení v produktu WebSphere Liberty (WLP), nemusí raději používat ukázky. WLP poskytuje další možnosti autorizace kromě těch, které jsou zde zdokumentovány.

Procedura

- Nakonfigurujte uživatele a skupiny se základním registrem pomocí souboru `basic_registry.xml` .

  Jména uživatelů a hesla v registru se používají k ověření a autorizaci uživatelů IBM MQ Console a REST API.

  Chcete-li nakonfigurovat základní registr pomocí ukázkového souboru `basic_registry.xml` , viz “Konfigurace základního registru pro IBM MQ Console a REST API” na stránce 528.
- Nakonfigurujte uživatele a skupiny s registrem LDAP pomocí souboru `ldap_registry.xml` .

  Jména uživatelů a hesla v registru LDAP se používají k ověření a autorizaci použití IBM MQ Console a REST API.

  Chcete-li konfigurovat registr LDAP pomocí ukázkového souboru `ldap_registry.xml` , prohlédněte si téma “Konfigurace registru LDAP pro IBM MQ Console a REST API” na stránce 533.
- ALW

  Nakonfigurujte uživatele a skupiny s registrem lokálního operačního systému pomocí souboru `local_os_registry.xml` .

  Jména uživatelů a hesla v registru operačního systému se používají k ověření a autorizaci uživatelů IBM MQ Console a REST API.

  Chcete-li konfigurovat lokální registr OS pomocí ukázkového souboru `local_os_registry.xml` , prohlédněte si téma “Konfigurace lokálního registru OS pro IBM MQ Console a REST API” na stránce 531.
- z/OS

  Konfigurujte uživatele a skupiny pomocí rozhraní SAF (System Authorization Facility) v systému z/OS pomocí souboru `zos_saf_registry.xml` .

Profily RACFnebo jiný produkt zabezpečení se používají k udělení přístupu uživatelů a skupin k rolím. Jména uživatelů a hesla v databázi RACF se používají k ověření a autorizaci uživatelů IBM MQ Console a REST API.

Chcete-li konfigurovat rozhraní SAF pomocí ukázkového souboru `zos_saf_registry.xml` , viz "Konfigurace registru SAF pro IBM MQ Console a REST API" na stránce 535.

- Zakažte zabezpečení, včetně schopnosti přistupovat k souboru IBM MQ Consolenebo k souboru REST APIpomocí protokolu HTTPS, pomocí souboru `no_security.xml` .

Jak pokračovat dále

Zvolte způsob ověřování uživatelů:

IBM MQ Console Volby ověření

- Umožnit uživatelům ověřit se pomocí ověření tokenu. V tomto případě uživatel zadá ID uživatele a heslo na přihlašovací obrazovce produktu IBM MQ Console . Je vygenerován token LTPA, který uživateli umožňuje zůstat přihlášený a autorizovaný po nastavenou dobu. Pro použití této volby ověřování není vyžadována žádná další konfigurace, můžete však volitelně konfigurovat interval vypršení platnosti pro token LTPA. Další informace naleznete v tématu Konfigurace intervalu vypršení platnosti tokenu LTPA.
- Umožnit uživatelům ověřit se pomocí certifikátů klienta. V tomto případě uživatel nepoužívá ID uživatele nebo heslo pro přihlášení k serveru IBM MQ Console, ale místo toho používá certifikát klienta. Další informace viz téma "Použití ověření pomocí certifikátu klienta s REST API a IBM MQ Console" na stránce 542.

REST API Volby ověření

- Umožnit uživatelům ověření pomocí základního ověření HTTP . V tomto případě je jméno uživatele a heslo zakódováno, ale není šifrováno, a odesláno s každým požadavkem REST API pro ověření a autorizaci uživatele pro tento požadavek. Aby bylo toto ověření zabezpečené, musíte použít zabezpečené připojení. To znamená, že musíte použít HTTPS. Další informace viz téma "Použití základního ověření HTTP s REST API" na stránce 546.
- Umožnit uživatelům ověřit se pomocí ověření tokenu. V tomto případě uživatel poskytne ID uživatele a heslo pro prostředek REST API `login` pomocí metody HTTP POST. Je vygenerován token LTPA, který uživateli umožňuje zůstat přihlášený a autorizovaný po nastavenou dobu. Další informace viz téma "Použití ověření založeného na tokenech s rozhraním REST API" na stránce 547. Můžete konfigurovat interval vypršení platnosti pro token LTPA. Další informace viz Konfigurace tokenu LTPA.
- Umožnit uživatelům ověřit se pomocí certifikátů klienta. V tomto případě uživatel nepoužívá ID uživatele nebo heslo pro přihlášení k serveru REST API, ale místo toho používá certifikát klienta. Další informace viz téma "Použití ověření pomocí certifikátu klienta s REST API a IBM MQ Console" na stránce 542.

Konfigurace základního registru pro IBM MQ Console a REST API

Základní registr můžete nakonfigurovat v souboru `mqwebuser.xml` . Jména uživatelů, hesla a role v souboru XML se používají k ověření a autorizaci uživatelů IBM MQ Console a REST API.

Než začnete

- Když konfigurujete uživatele v základním registru, musíte každému uživateli přiřadit roli. Každá role poskytuje různé úrovně oprávnění pro přístup k funkcím IBM MQ Console a REST APIa určuje kontext zabezpečení, který se používá při pokusu o provedení povolené operace. Před konfigurací základního registru musíte těmto rolím porozumět. Další informace o jednotlivých rolích viz "Role na IBM MQ Console a REST API" na stránce 537.
- Chcete-li dokončit tuto úlohu, musíte být uživatel s dostatečnými oprávněními k úpravě souboru `mqwebuser.xml` :

– z/OS V systému z/OSmusíte mít přístup pro zápis do souboru `mqwebuser.xml` .

– Multi U všech ostatních operačních systémů musíte být privilegovaný uživatel.

– V 9.3.5 Linux Pokud je server mqweb součástí samostatné instalace produktu IBM MQ Web Server , musíte mít přístup pro zápis k souboru `mqwebuser.xml` v datovém adresáři IBM MQ Web Server .

Postup

1. Zkopírujte ukázkový soubor XML `basic_registry.xml` z jedné z následujících cest:
   - V instalaci produktu IBM MQ :
     – ALW V systému AIX, Linux, and Windows: *MQ_INSTALLATION_PATH* `/web/mq/samp/configuration`
     – z/OS V systému z/OS: `PathPrefix /web/mq/samp/configuration`

     kde `PathPrefix` je instalační cesta IBM MQ for z/OS UNIX System Services Components .
   - V 9.3.5 Linux V samostatné IBM MQ Web Server instalaci: *MQWEB_INSTALLATION_PATH*`/web/mq/samp/configuration`

     kde *MQWEB_INSTALLATION_PATH* je adresář, do kterého byl dekomprimován instalační soubor IBM MQ Web Server .
2. Umístěte ukázkový soubor do příslušného adresáře:
   - V instalaci produktu IBM MQ :
     – Linux AIX V systému AIX nebo Linux: `/var/mqm/web/installations/`*`installationName`*`/servers/mqweb`
     – Windows V systému Windows: *MQ_DATA_PATH*`\web\installations\`*`installationName`*`\servers\mqweb`, kde *MQ_DATA_PATH* je cesta k datům IBM MQ . Tato cesta je cestou k datům, která je vybrána během instalace produktu IBM MQ. Standardně je tato cesta `C:\ProgramData\IBM\MQ`.
     – z/OS V systému z/OS: *WLP_user_directory*`/servers/mqweb`

     kde *WLP_user_directory* je adresář určený při spuštění skriptu **crtmqweb** za účelem vytvoření definice serveru mqweb.
   - V 9.3.5 Linux V samostatné IBM MQ Web Server instalaci: *MQ_OVERRIDE_DATA_PATH*`/web/installations/MQWEBINST/servers/mqweb`

     kde *MQ_OVERRIDE_DATA_PATH* je datový adresář IBM MQ Web Server , na který odkazuje proměnná prostředí **MQ_OVERRIDE_DATA_PATH** .
3. Volitelné: Pokud jste změnili některá nastavení konfigurace v souboru `mqwebuser.xml`, zkopírujte je do ukázkového souboru.
4. Odstraňte existující soubor `mqwebuser.xml` a přejmenujte ukázkový soubor na `mqwebuser.xml`.
5. Upravte nový soubor `mqwebuser.xml` a přidejte uživatele a skupiny v rámci značek **basicRegistry** .

   Mějte na paměti, že každý uživatel s rolí `MQWebUser` může provádět pouze operace, které je ID uživatele uděleno k provedení ve správci front. Proto musí mít ID uživatele definované v registru identické ID uživatele na systému, na kterém je nainstalován produkt IBM MQ . Tato ID uživatelů musí být ve stejném případě, jinak může dojít k selhání mapování mezi ID uživatelů.

   Další informace o konfiguraci základních registrů uživatelů viz téma Konfigurace základního registru uživatelů pro Liberty v dokumentaci WebSphere Liberty .
6. Přiřaďte role uživatelům a skupinám úpravou souboru `mqwebuser.xml` :

K dispozici je několik rolí, které autorizují uživatele a skupiny k použití konzoly IBM MQ Consolea konzoly REST API. Každá role uděluje jinou úroveň přístupu. Další informace viz téma “Role na IBM MQ Console a REST API” na stránce 537.

- Chcete-li přiřadit role a udělit přístup k produktu IBM MQ Console, přidejte své uživatele a skupiny mezi příslušné značky **security-role** v rámci značek **<enterpriseApplication id="com.ibm.mq.console">** .
- Chcete-li přiřadit role a udělit přístup k produktu REST API, přidejte své uživatele a skupiny mezi příslušné značky **security-role** v rámci značek **<enterpriseApplication id="com.ibm.mq.rest">** .

Nápovědu k formátu informací o uživatelích a skupinách v rámci značek **security-role** naleznete v příkladech.

7. Pokud jste zadali hesla pro uživatele v produktu `mqwebuser.xml`, měli byste tato hesla zakódovat, aby byla bezpečnější, pomocí příkazu **securityUtility encoding** poskytnutého produktem WebSphere Liberty. Další informace viz Liberty: příkazsecurityUtility v dokumentaci k produktu WebSphere Liberty .

Příklad

V následujícím příkladu je skupině `MQWebAdminGroup` udělen přístup k IBM MQ Console s rolí `MQWebAdmin`. Uživateli `reader`je udělen přístup s rolí `MQWebAdminRO`a uživateli `guest` je udělen přístup s rolí `MQWebUser`:

```
<enterpriseApplication id="com.ibm.mq.console">
        <application-bnd>
            <security-role name="MQWebAdmin">
                <group name="MQWebAdminGroup" realm="defaultRealm"/>
            </security-role>
            <security-role name="MQWebAdminRO">
                <user name="reader" realm="defaultRealm"/>
            </security-role>
            <security-role name="MQWebUser">
                <user name="guest" realm="defaultRealm"/>
            </security-role>
        </application-bnd>
    </enterpriseApplication>
```

V následujícím příkladu jsou uživatelům `reader` a `guest` udělen přístup k souboru IBM MQ Console. Uživateli `user` je udělen přístup k produktu REST APIa všem uživatelům ve skupině `MQAdmin` je udělen přístup k IBM MQ Console a REST API. Uživateli `mftadmin` je udělen přístup k souboru REST API pro MFT :

```
<enterpriseApplication id="com.ibm.mq.console">
    <application-bnd>
        <security-role name="MQWebAdmin">
            <group name="MQAdmin" realm="defaultRealm"/>
        </security-role>
        <security-role name="MQWebAdminRO">
            <user name="reader" realm="defaultRealm"/>
        </security-role>
        <security-role name="MQWebUser">
            <user name="guest" realm="defaultRealm"/>
        </security-role>
    </application-bnd>
</enterpriseApplication>

<enterpriseApplication id="com.ibm.mq.rest">
    <application-bnd>
        <security-role name="MQWebAdmin">
            <group name="MQAdmin" realm="defaultRealm"/>
        </security-role>
        <security-role name="MQWebUser">
            <user name="user" realm="defaultRealm"/>
        </security-role>
        <security-role name="MFTWebAdmin">
            <user name="mftadmin" realm="defaultRealm"/>
        </security-role>
     </application-bnd>
</enterpriseApplication>
```

Jak pokračovat dále

Zvolte způsob ověřování uživatelů:

IBM MQ Console Volby ověření

- Umožnit uživatelům ověřit se pomocí ověření tokenu. V tomto případě uživatel zadá ID uživatele a heslo na přihlašovací obrazovce produktu IBM MQ Console . Je vygenerován token LTPA, který uživateli umožňuje zůstat přihlášený a autorizovaný po nastavenou dobu. Pro použití této volby ověřování není vyžadována žádná další konfigurace, můžete však volitelně konfigurovat interval vypršení platnosti pro token LTPA. Další informace naleznete v tématu Konfigurace intervalu vypršení platnosti tokenu LTPA.
- Umožnit uživatelům ověřit se pomocí certifikátů klienta. V tomto případě uživatel nepoužívá ID uživatele nebo heslo pro přihlášení k serveru IBM MQ Console, ale místo toho používá certifikát klienta. Další informace viz téma “Použití ověření pomocí certifikátu klienta s REST API a IBM MQ Console” na stránce 542.

REST API Volby ověření

- Umožnit uživatelům ověření pomocí základního ověření HTTP . V tomto případě je jméno uživatele a heslo zakódováno, ale není šifrováno, a odesláno s každým požadavkem REST API pro ověření a autorizaci uživatele pro tento požadavek. Aby bylo toto ověření zabezpečené, musíte použít zabezpečené připojení. To znamená, že musíte použít HTTPS. Další informace viz téma “Použití základního ověření HTTP s REST API” na stránce 546.
- Umožnit uživatelům ověřit se pomocí ověření tokenu. V tomto případě uživatel poskytne ID uživatele a heslo pro prostředek REST API `login` pomocí metody HTTP POST. Je vygenerován token LTPA, který uživateli umožňuje zůstat přihlášený a autorizovaný po nastavenou dobu. Další informace viz téma “Použití ověření založeného na tokenech s rozhraním REST API” na stránce 547. Můžete konfigurovat interval vypršení platnosti pro token LTPA. Další informace viz Konfigurace tokenu LTPA.
- Umožnit uživatelům ověřit se pomocí certifikátů klienta. V tomto případě uživatel nepoužívá ID uživatele nebo heslo pro přihlášení k serveru REST API, ale místo toho používá certifikát klienta. Další informace viz téma “Použití ověření pomocí certifikátu klienta s REST API a IBM MQ Console” na stránce 542.

ALW Konfigurace lokálního registru OS pro IBM MQ Console a REST API

Registr lokálního operačního systému můžete nakonfigurovat v souboru `mqwebuser.xml` . Jména uživatelů a hesla v lokálním operačním systému se používají k ověření a autorizaci uživatelů serveru IBM MQ Console a serveru REST API.

Než začnete

- Pro ověření pomocí certifikátu klienta s funkcí ověření lokálního operačního systému je identita uživatele obecný název (CN) z rozlišujícího názvu (DN) certifikátu klienta. Pokud identita uživatele neexistuje jako uživatel operačního systému, přihlášení pomocí certifikátu klienta selže a provede se návrat k ověření založenému na hesle.
- Chcete-li dokončit tuto úlohu, musíte být uživatel s dostatečnými oprávněními k úpravě souboru `mqwebuser.xml` :
  - V 9.3.5 Linux Pokud je server mqweb součástí samostatné instalace produktu IBM MQ Web Server , musíte mít přístup pro zápis k souboru `mqwebuser.xml` v datovém adresáři IBM MQ Web Server .
  - Pokud je server mqweb součástí instalace produktu IBM MQ , musíte být privilegovaný uživatel.

Informace o této úloze

V registru lokálního operačního systému jsou uživatelům a skupinám automaticky přiřazena role:

- Každému uživateli, který je součástí skupiny 'mqm' nebo skupiny 'QMQMADM' v systému IBM i, jsou uděleny role `MQWebAdmin` a `MFTWebAdmin` .
- Všem ostatním uživatelům je udělena role `MQWebUser` .

Další informace o těchto rolích viz “Role na IBM MQ Console a REST API” na stránce 537.

Registr lokálního operačního systému lze použít pouze v systému AIX, Linux, and Windows. Ekvivalentní funkce je poskytována v systému z/OS konfigurací registru SAF. Další informace viz téma “Konfigurace registru SAF pro IBM MQ Console a REST API” na stránce 535.

Postup

1. Zkopírujte ukázkový soubor XML `local_os_registry.xml` z jedné z následujících cest:
   - V 9.3.5 Linux V samostatné IBM MQ Web Server instalaci: *MQWEB_INSTALLATION_PATH*`/web/mq/samp/configuration`

     kde *MQWEB_INSTALLATION_PATH* je adresář, do kterého byl dekomprimován instalační soubor IBM MQ Web Server .
   - V IBM MQ instalaci: *MQ_INSTALLATION_PATH*`/web/mq/samp/configuration`
2. Umístěte ukázkový soubor do jednoho z následujících adresářů:
   - V 9.3.5 Linux V samostatné IBM MQ Web Server instalaci: *MQ_OVERRIDE_DATA_PATH*`/web/installations/MQWEBINST/servers/mqweb`

     kde *MQ_OVERRIDE_DATA_PATH* je datový adresář IBM MQ Web Server , na který odkazuje proměnná prostředí **MQ_OVERRIDE_DATA_PATH** .
   - V IBM MQ instalaci: *MQ_DATA_PATH*`/web/installations/`*installationName*`/servers/mqweb`
3. Volitelné: Pokud jste změnili některá nastavení konfigurace v souboru `mqwebuser.xml`, zkopírujte je do ukázkového souboru.
4. Odstraňte existující soubor `mqwebuser.xml` a přejmenujte ukázkový soubor na `mqwebuser.xml`.

Jak pokračovat dále

Zvolte způsob ověřování uživatelů:

IBM MQ Console Volby ověření

- Umožnit uživatelům ověřit se pomocí ověření tokenu. V tomto případě uživatel zadá ID uživatele a heslo na přihlašovací obrazovce produktu IBM MQ Console . Je vygenerován token LTPA, který uživateli umožňuje zůstat přihlášený a autorizovaný po nastavenou dobu. Pro použití této volby ověřování není vyžadována žádná další konfigurace, můžete však volitelně konfigurovat interval vypršení platnosti pro token LTPA. Další informace naleznete v tématu Konfigurace intervalu vypršení platnosti tokenu LTPA.
- Umožnit uživatelům ověřit se pomocí certifikátů klienta. V tomto případě uživatel nepoužívá ID uživatele nebo heslo pro přihlášení k serveru IBM MQ Console, ale místo toho používá certifikát klienta. Další informace viz téma “Použití ověření pomocí certifikátu klienta s REST API a IBM MQ Console” na stránce 542.

REST API Volby ověření

- Umožnit uživatelům ověření pomocí základního ověření HTTP . V tomto případě je jméno uživatele a heslo zakódováno, ale není šifrováno, a odesláno s každým požadavkem REST API pro ověření a autorizaci uživatele pro tento požadavek. Aby bylo toto ověření zabezpečené, musíte použít zabezpečené připojení. To znamená, že musíte použít HTTPS. Další informace viz téma “Použití základního ověření HTTP s REST API” na stránce 546.
- Umožnit uživatelům ověřit se pomocí ověření tokenu. V tomto případě uživatel poskytne ID uživatele a heslo pro prostředek REST API `login` pomocí metody HTTP POST. Je vygenerován token LTPA,

který uživateli umožňuje zůstat přihlášený a autorizovaný po nastavenou dobu. Další informace viz téma “Použití ověření založeného na tokenech s rozhraním REST API” na stránce 547. Můžete konfigurovat interval vypršení platnosti pro token LTPA. Další informace viz Konfigurace tokenu LTPA.

- Umožnit uživatelům ověřit se pomocí certifikátů klienta. V tomto případě uživatel nepoužívá ID uživatele nebo heslo pro přihlášení k serveru REST API, ale místo toho používá certifikát klienta. Další informace viz téma “Použití ověření pomocí certifikátu klienta s REST API a IBM MQ Console” na stránce 542.

Konfigurace registru LDAP pro IBM MQ Console a REST API

Registr LDAP můžete nakonfigurovat v souboru `mqwebuser.xml` . Jména uživatelů a hesla v registru LDAP se používají k ověření a autorizaci uživatelů IBM MQ Console a REST API.

Než začnete

- Když konfigurujete registr LDAP, musíte každému uživateli přiřadit roli. Každá role poskytuje různé úrovně oprávnění pro přístup k funkcím IBM MQ Console a REST APIa určuje kontext zabezpečení, který se používá při pokusu o provedení povolené operace. Před konfigurací registru musíte těmto rolím porozumět. Další informace o jednotlivých rolích viz “Role na IBM MQ Console a REST API” na stránce 537.

  Mějte na paměti, že každý uživatel s rolí `MQWebUser` může provádět pouze operace, které je ID uživatele uděleno k provedení ve správci front. Proto musí mít ID uživatele definované na serveru LDAP identické ID uživatele na systému, na kterém je nainstalován produkt IBM MQ . Tato ID uživatelů musí být ve stejném případě, jinak může dojít k selhání mapování mezi ID uživatelů.
- Chcete-li dokončit tuto úlohu, musíte být uživatel s dostatečnými oprávněními k úpravě souboru `mqwebuser.xml` :
  - z/OS V systému z/OSmusíte mít přístup pro zápis do souboru `mqwebuser.xml` .
  - Multi U všech ostatních operačních systémů musíte být privilegovaný uživatel.
  - V 9.3.5 Linux Pokud je server mqweb součástí samostatné instalace produktu IBM MQ Web Server , musíte mít přístup pro zápis k souboru `mqwebuser.xml` v datovém adresáři IBM MQ Web Server .

Postup

1. Zkopírujte ukázkový soubor XML `ldap_registry.xml` z jedné z následujících cest:
   - V instalaci produktu IBM MQ :
     - ALW V systému AIX, Linux, and Windows: *MQ_INSTALLATION_PATH* `/web/mq/samp/configuration`
     - z/OS V systému z/OS: `PathPrefix /web/mq/samp/configuration`

       kde `PathPrefix` je instalační cesta IBM MQ for z/OS UNIX System Services Components .
   - V 9.3.5 Linux V samostatné IBM MQ Web Server instalaci: *MQWEB_INSTALLATION_PATH*`/web/mq/samp/configuration`

     kde *MQWEB_INSTALLATION_PATH* je adresář, do kterého byl dekomprimován instalační soubor IBM MQ Web Server .
2. Umístěte ukázkový soubor do příslušného adresáře:
   - V instalaci produktu IBM MQ :
     - Linux AIX V systému AIX nebo Linux: `/var/mqm/web/installations/`*installationName*`/servers/mqweb`

– Windows V systému Windows: *MQ_DATA_PATH*\web\installations*installationName*\servers\mqweb, kde *MQ_DATA_PATH* je cesta k datům IBM MQ . Tato cesta je cestou k datům, která je vybrána během instalace produktu IBM MQ. Standardně je tato cesta C:\ProgramData\IBM\MQ.

– z/OS V systému z/OS: *WLP_user_directory*/servers/mqweb

kde *WLP_user_directory* je adresář určený při spuštění skriptu **crtmqweb** za účelem vytvoření definice serveru mqweb.

- V 9.3.5 Linux V samostatné IBM MQ Web Server instalaci: *MQ_OVERRIDE_DATA_PATH*/web/installations/MQWEBINST/servers/mqweb

  kde *MQ_OVERRIDE_DATA_PATH* je datový adresář IBM MQ Web Server , na který odkazuje proměnná prostředí **MQ_OVERRIDE_DATA_PATH** .

3. Volitelné: Pokud jste změnili některá nastavení konfigurace v souboru mqwebuser.xml, zkopírujte je do ukázkového souboru.
4. Odstraňte existující soubor mqwebuser.xml a přejmenujte ukázkový soubor na mqwebuser.xml.
5. Upravte nový soubor mqwebuser.xml a změňte nastavení registru LDAP v rámci značek **ldapRegistry** a **idsLdapFilterProperties** .

   Další informace o konfiguraci registrů LDAP viz Konfigurace registrů uživatelů LDAP v Liberty v dokumentaci WebSphere Liberty .
6. Přiřaďte role uživatelům a skupinám úpravou souboru mqwebuser.xml :

   K dispozici je několik rolí, které autorizují uživatele a skupiny k použití konzoly IBM MQ Consolea konzoly REST API. Každá role uděluje jinou úroveň přístupu. Další informace viz téma “Role na IBM MQ Console a REST API” na stránce 537.

   - Chcete-li přiřadit role a udělit přístup k produktu IBM MQ Console, přidejte své uživatele a skupiny mezi příslušné značky **security-role** v rámci značek **<enterpriseApplication id="com.ibm.mq.console">** .
   - Chcete-li přiřadit role a udělit přístup k produktu REST API, přidejte své uživatele a skupiny mezi příslušné značky **security-role** v rámci značek **<enterpriseApplication id="com.ibm.mq.rest">** .

Jak pokračovat dále

Zvolte způsob ověřování uživatelů:

IBM MQ Console Volby ověření

- Umožnit uživatelům ověřit se pomocí ověření tokenu. V tomto případě uživatel zadá ID uživatele a heslo na přihlašovací obrazovce produktu IBM MQ Console . Je vygenerován token LTPA, který uživateli umožňuje zůstat přihlášený a autorizovaný po nastavenou dobu. Pro použití této volby ověřování není vyžadována žádná další konfigurace, můžete však volitelně konfigurovat interval vypršení platnosti pro token LTPA. Další informace naleznete v tématu Konfigurace intervalu vypršení platnosti tokenu LTPA.
- Umožnit uživatelům ověřit se pomocí certifikátů klienta. V tomto případě uživatel nepoužívá ID uživatele nebo heslo pro přihlášení k serveru IBM MQ Console, ale místo toho používá certifikát klienta. Další informace viz téma “Použití ověření pomocí certifikátu klienta s REST API a IBM MQ Console” na stránce 542.

REST API Volby ověření

- Umožnit uživatelům ověření pomocí základního ověření HTTP . V tomto případě je jméno uživatele a heslo zakódováno, ale není šifrováno, a odesláno s každým požadavkem REST API pro ověření a autorizaci uživatele pro tento požadavek. Aby bylo toto ověření zabezpečené, musíte použít zabezpečené připojení. To znamená, že musíte použít HTTPS. Další informace viz téma “Použití základního ověření HTTP s REST API” na stránce 546.

- Umožnit uživatelům ověřit se pomocí ověření tokenu. V tomto případě uživatel poskytne ID uživatele a heslo pro prostředek REST API `login` pomocí metody HTTP POST. Je vygenerován token LTPA, který uživateli umožňuje zůstat přihlášený a autorizovaný po nastavenou dobu. Další informace viz téma “Použití ověření založeného na tokenech s rozhraním REST API” na stránce 547. Můžete konfigurovat interval vypršení platnosti pro token LTPA. Další informace viz Konfigurace tokenu LTPA.
- Umožnit uživatelům ověřit se pomocí certifikátů klienta. V tomto případě uživatel nepoužívá ID uživatele nebo heslo pro přihlášení k serveru REST API, ale místo toho používá certifikát klienta. Další informace viz téma “Použití ověření pomocí certifikátu klienta s REST API a IBM MQ Console” na stránce 542.

z/OS Konfigurace registru SAF pro IBM MQ Console a REST API

Rozhraní SAF (System Authorization Facility) umožňuje serveru mqweb volat externího správce zabezpečení pro ověřování a kontrolu autorizace. Uživatel se pak může přihlásit k IBM MQ Console a REST API pomocí ID a hesla uživatele z/OS .

Než začnete

- Při konfiguraci registru SAF musíte přiřadit uživatelům roli. Každá role poskytuje různé úrovně oprávnění pro přístup k funkcím IBM MQ Console a REST APIa určuje kontext zabezpečení, který se používá při pokusu o provedení povolené operace. Před konfigurací registru musíte těmto rolím porozumět. Další informace o jednotlivých rolích viz “Role na IBM MQ Console a REST API” na stránce 537.
- Chcete-li používat autorizované rozhraní pro zařízení SAF, musíte spustit proces WebSphere Liberty Angel. Další informace viz Povolení autorizovaných služeb z/OS na serveru Liberty for z/OS .
- Chcete-li dokončit tuto úlohu, musíte mít přístup pro zápis k souboru `mqwebuser.xml` a oprávnění k definování profilů správce zabezpečení.

Poznámka: V 9.3.5 V 9.3.0.20 Z IBM MQ 9.3.5 pro Continuous Delivery a z IBM MQ 9.3.0 Fix Pack 20 pro Long Term Supportbyl ukázkový konfigurační soubor `zos_saf_registry.xml` aktualizován, aby odebral duplicitní položku safAuthorization .

Tato aktualizace opravuje problém, kde se může vyskytnout chyba ICH408I , když se IBM MQ Console na z/OS upgraduje na úroveň, která se dodává WebSphere Liberty Profile 22.0.0.12 nebo novější: to znamená z IBM MQ 9.3.0 Fix Pack 2 pro Long Term Support a z IBM MQ 9.3.1 CSU 1 a IBM MQ 9.3.2 pro Continuous Delivery. Použití více než jednoho příkazu safAuthorization není podporováno a může způsobit chybu ICH408I v případě, že uživatelé, kteří nejsou v rolích MQWebAdmin nebo MQWebAdminRO ve třídě EBJROLE, se pokusí o přístup ke správci front z/OS prostřednictvím konzoly IBM MQ Console.

Výchozí hodnota parametru **`racRouteLog`**, která určuje typy pokusů o přístup k protokolu, je `NONE`. Pokud potřebujete další sestavu nebo záznam pro auditování zabezpečení, další informace naleznete v tématu Autorizace SAF (safAuthorization) .

Informace o této úloze

Rozhraní SAF umožňuje serveru mqweb volat externího správce zabezpečení pro ověření a kontrolu autorizace pro IBM MQ Console i REST API.

Postup

1. Postupujte podle pokynů v části Povolení autorizovaných služeb z/OS na serveru Liberty for z/OS , abyste poskytli svému serveru mqweb přístup k použití autorizovaných služeb z/OS .

   Ukázkový soubor JCL pro spuštění procesu typu angel je v adresáři USS_ROOT/web/`templates/zos/procs/bbgzangl.jcl`, kde USS_ROOT je cesta v adresáři z/OS UNIX System Services (z/OS UNIX), kde jsou nainstalovány komponenty z/OS UNIX .

   V souboru `bbgzangl.jcl`změňte příkaz SET ROOT tak, aby ukazoval na USS_ROOT/web, například `/usr/lpp/mqm/V9R2M0/web`.

Další informace o zastavení a spuštění procesu typu angel viz Administrace Liberty v systému z/OS .

2. Postupujte podle pokynů v části Liberty: Nastavení neověřeného uživatele SAF (System Authorization Facility) a vytvořte neověřeného uživatele, kterého produkt Libertypotřebuje.
3. Zkopírujte soubor `zos_saf_registry.xml` z následující cesty: `PathPrefix /web/mq/samp/configuration` , kde `PathPrefix` je instalační cesta ke komponentám z/OS UNIX .
4. Umístěte ukázkový soubor do adresáře *WLP_user_directory*`/servers/mqweb` , kde *WLP_user_directory* je adresář určený při spuštění skriptu **crtmqweb** pro vytvoření definice serveru mqweb.
5. Volitelné: Pokud jste dříve změnili některá nastavení konfigurace v souboru `mqwebuser.xml`, zkopírujte je do ukázkového souboru.
6. Odstraňte existující soubor `mqwebuser.xml` a přejmenujte ukázkový soubor na `mqwebuser.xml`.
7. Upravte prvek **safCredentials** v souboru `mqwebuser.xml`.
   a. Nastavte **profilePrefix** na název, který je jedinečný pro váš server Liberty. Pokud je v jednom systému spuštěn více než jeden server mqweb, je třeba pro každý server zvolit jiný název, například MQWEB920 a MQWEB915.
   b. Nastavte **unauthenticatedUser** na jméno neověřeného uživatele vytvořeného v kroku “2” na stránce 536.
8. Definujte parametr APPLID serveru mqweb na hodnotu RACF.

   Název prostředku APPLID je hodnota, kterou jste zadali v atributu **profilePrefix** v kroku “7” na stránce 536. Následující příklad definuje identifikátor APPLID serveru mqweb v adresáři RACF:

   ```
   RDEFINE APPL profilePrefix UACC(NONE)
   ```

9. Udělte všem uživatelům nebo skupinám oprávnění k ověření přístupu IBM MQ Console nebo REST API READ k serveru mqweb APPLID ve třídě APPL.

   To musíte provést i pro neověřeného uživatele definovaného v kroku “2” na stránce 536. Následující příklad udělí uživateli přístup pro čtení (READ) k serveru mqweb APPLID v adresáři RACF:

   ```
   PERMIT profilePrefix CLASS(APPL) ACCESS(READ) ID(userID)
   ```

10. Pomocí příkazu **SETROPTS** RACF obnovte profily tříd RACLISTed APPL v úložišti:

    ```
    SETROPTS RACLIST(APPL) REFRESH
    ```

11. Definujte profily ve třídě EJBROLE potřebné k tomu, aby měli uživatelé přístup k rolím v adresáři IBM MQ Console a REST API.

    Následující příklad definuje profily v souboru RACF, kde **profilePrefix** je hodnota určená pro atribut **profilePrefix** v kroku “7” na stránce 536.

```
RDEFINE EJBROLE profilePrefix.com.ibm.mq.console.MQWebAdmin UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.console.MQWebAdminRO UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.console.MQWebUser UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.rest.MQWebAdmin UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.rest.MQWebAdminRO UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.rest.MQWebUser UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.rest.MFTWebAdmin UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.rest.MFTWebAdminRO UACC(NONE)
```

12. Udělte uživatelům přístup k rolím v IBM MQ Console a REST API.

    Chcete-li tak učinit, udělte uživatelům nebo skupinám přístup pro čtení k jednomu nebo více profilům ve třídě EBJROLE vytvořené v kroku “11” na stránce 536. Další informace o rolích viz “Role na IBM MQ Console a REST API” na stránce 537.

    Následující příklad poskytuje uživateli přístup k roli MQWebAdmin pro REST API in RACF, kde **profilePrefix** je hodnota určená pro atribut **profilePrefix** v kroku “7” na stránce 536.

```
PERMIT profilePrefix.com.ibm.mq.rest.MQWebAdmin CLASS(EJBROLE) ACCESS(READ) ID(userID)
```

Výsledky

Nastavili jste ověřování SAF pro zařízení IBM MQ Console a REST API.

Jak pokračovat dále

Zvolte způsob ověřování uživatelů:

IBM MQ Console Volby ověření

- Umožnit uživatelům ověřit se pomocí ověření tokenu. V tomto případě uživatel zadá ID uživatele a heslo na přihlašovací obrazovce produktu IBM MQ Console . Je vygenerován token LTPA, který uživateli umožňuje zůstat přihlášený a autorizovaný po nastavenou dobu. Pro použití této volby ověřování není vyžadována žádná další konfigurace, můžete však volitelně konfigurovat interval vypršení platnosti pro token LTPA. Další informace naleznete v tématu Konfigurace intervalu vypršení platnosti tokenu LTPA.
- Umožnit uživatelům ověřit se pomocí certifikátů klienta. V tomto případě uživatel nepoužívá ID uživatele nebo heslo pro přihlášení k serveru IBM MQ Console, ale místo toho používá certifikát klienta. Další informace viz téma “Použití ověření pomocí certifikátu klienta s REST API a IBM MQ Console” na stránce 542.

REST API Volby ověření

- Umožnit uživatelům ověření pomocí základního ověření HTTP . V tomto případě je jméno uživatele a heslo zakódováno, ale není šifrováno, a odesláno s každým požadavkem REST API pro ověření a autorizaci uživatele pro tento požadavek. Aby bylo toto ověření zabezpečené, musíte použít zabezpečené připojení. To znamená, že musíte použít HTTPS. Další informace viz téma “Použití základního ověření HTTP s REST API” na stránce 546.
- Umožnit uživatelům ověřit se pomocí ověření tokenu. V tomto případě uživatel poskytne ID uživatele a heslo pro prostředek REST API `login` pomocí metody HTTP POST. Je vygenerován token LTPA, který uživateli umožňuje zůstat přihlášený a autorizovaný po nastavenou dobu. Další informace viz téma “Použití ověření založeného na tokenech s rozhraním REST API” na stránce 547. Můžete konfigurovat interval vypršení platnosti pro token LTPA. Další informace viz Konfigurace tokenu LTPA.
- Umožnit uživatelům ověřit se pomocí certifikátů klienta. V tomto případě uživatel nepoužívá ID uživatele nebo heslo pro přihlášení k serveru REST API, ale místo toho používá certifikát klienta. Další informace viz téma “Použití ověření pomocí certifikátu klienta s REST API a IBM MQ Console” na stránce 542.

Role na IBM MQ Console a REST API

Když autorizujete uživatele a skupiny k použití IBM MQ Console nebo REST API, musíte přiřadit uživatelům a skupinám jednu z dostupných rolí: **MQWebAdmin**, **MQWebAdminRO**, **MQWebUser**, **MFTWebAdmin**a **MFTWebAdminRO**. Každá role poskytuje různé úrovně oprávnění pro přístup k funkcím IBM MQ Console a REST APIa určuje kontext zabezpečení, který se používá při pokusu o provedení povolené operace.

Poznámka: S výjimkou role **MQWebUser** ID uživatele nerozlišuje velikost písmen. Specifické požadavky pro tuto roli viz “MQWebUser” na stránce 538 .

MQWebAdmin
Uživatel nebo skupina, které je přiřazena tato role, může provádět všechny administrativní operace a pracovat v kontextu zabezpečení ID uživatele operačního systému, které se používá ke spuštění serveru mqweb.

Uživatel nebo skupina s touto rolí nemá přístup k následujícím službám REST:

- REST API pro MFT. Chcete-li tyto služby používat, musí být uživateli nebo skupině také přiřazena role **MFTWebAdmin** nebo **MFTWebAdminRO** .
- Soubor messaging REST API. Chcete-li použít messaging REST API, musí být uživateli přiřazena role **MQWebUser** .

MQWebAdminRO
Tato role poskytuje přístup jen pro čtení k serveru IBM MQ Console nebo REST API. Uživatel nebo skupina, které je přiřazena tato role, může provádět následující operace:

- Zobrazit a zjistit operace na objektech IBM MQ , jako jsou fronty a kanály.
- Procházet zprávy ve frontách.

Uživatel nebo skupina, které je přiřazena tato role, pracuje v kontextu zabezpečení ID uživatele operačního systému, které se používá ke spuštění serveru mqweb.

Uživatel nebo skupina s touto rolí nemá přístup k následujícím službám REST:

- REST API pro MFT. Chcete-li tyto služby používat, musí být uživateli nebo skupině také přiřazena role **MFTWebAdmin** nebo **MFTWebAdminRO** .
- Soubor messaging REST API. Chcete-li použít messaging REST API, musí být uživateli přiřazena role **MQWebUser** .

MQWebUser
Uživatel nebo skupina, které je přiřazena tato role, může provést libovolnou operaci, které je ID uživatele uděleno k provedení ve správci front. Příklad:

- Spusťte a zastavte operace na objektech IBM MQ , jako jsou kanály.
- Definujte a nastavte operace na objektech IBM MQ , jako jsou fronty a kanály.
- Zobrazit a zjistit operace na objektech IBM MQ , jako jsou fronty a kanály.
- Vložte a získejte zprávy pomocí konzoly messaging REST API.

Uživatel nebo skupina, které je přiřazena tato role, pracuje v kontextu zabezpečení činitele a může provádět pouze operace, kterým je ID uživatele uděleno pro provedení ve správci front.

Proto musí být uživateli nebo skupině, která je definována v registru uživatelů mqweb, uděleno oprávnění v rámci produktu IBM MQ , aby mohl tento uživatel provádět jakékoli operace. Pomocí této role můžete jemně řídit, kteří uživatelé mají typ přístupu ke specifickým prostředkům IBM MQ , když používají prostředky IBM MQ Console a REST API.

Poznámka:

- Maximální délka ID uživatele, kterému je přiřazena tato role, je 12 znaků.
- Případ ID uživatele musí být stejný v registru uživatelů mqweb a v systému IBM MQ . Pokud je případ ID uživatele jiný, uživatel může být ověřen pomocí IBM MQ Console a REST API , ale nemá oprávnění používat prostředky IBM MQ .

MFTWebAdmin
Uživatel nebo skupina s touto rolí může provádět všechny operace REST produktu MFT a pracovat v kontextu zabezpečení ID uživatele operačního systému, které se používá ke spuštění serveru mqweb .

Uživatel nebo skupina s touto rolí nemá přístup k žádné ze služeb produktu IBM MQ REST API . Chcete-li tyto služby používat, musí být uživateli nebo skupině také přiřazena role **MQWebAdmin**, **MQWebAdminRO**nebo **MQWebUser** .

MFTWebAdminRO
Tato role poskytuje přístup jen pro čtení k REST API pro MFT . Uživatel nebo skupina, které je přiřazena tato role, může provádět operace jen pro čtení (požadavky GET), jako např. přenos seznamu a agenti seznamu.

Uživatel nebo skupina, které je přiřazena tato role, pracuje v kontextu zabezpečení ID uživatele operačního systému, které se používá ke spuštění serveru mqweb.

Uživatel nebo skupina s touto rolí nemá přístup k žádné ze služeb produktu IBM MQ REST API . Chcete-li tyto služby používat, musí být uživateli nebo skupině také přiřazena role **MQWebAdmin**, **MQWebAdminRO**nebo **MQWebUser** .

Další informace o konfiguraci uživatelů a skupin pro použití těchto rolí viz "Konfigurace uživatelů a rolí" na stránce 527.

Překrývající se role

Uživateli nebo skupině lze přiřadit více než jednu roli. Když uživatel provede operaci v této situaci, použije se nejvyšší role oprávnění, která je použitelná pro operaci. Pokud například uživatel s rolemi **MQWebAdminRO** a **MQWebUser** provede operaci dotazování fronty, použije se role **MQWebAdminRO** a operace se provede pod kontextem ID uživatele systému, který spustil webový server. Pokud stejný uživatel provede operaci definice, použije se role **MQWebUser** a operace se provede pod kontextem činitele.

ALW Změna certifikátu poskytnutého produktem IBM MQ Console do prohlížeče

Produkt IBM MQ Console můžete nakonfigurovat tak, aby prezentoval vlastní certifikát podepsaný certifikační autoritou pro účely ověření. Tím se odebere varování certifikátu podepsaného svým držitelem, které představuje webový prohlížeč při přístupu ke konzole IBM MQ Console .

Než začnete

Nakonfigurujte uživatele, skupiny a role, které mají být autorizovány k použití produktu IBM MQ Console. Další informace viz téma “Konfigurace uživatelů a rolí” na stránce 527.

Informace o této úloze

Zabezpečení konzoly je poskytováno produktem IBM WebSphere Application Server Liberty používaným vaší instalací produktu IBM MQ .

Chcete-li změnit certifikát, který tento server předkládá vašemu prohlížeči, musíte:

1. Přidejte certifikát, který chcete prezentovat, do úložiště klíčů webového serveru.
2. Popište certifikát.
3. Upravte soubor `mqwebuser.xml` a vypněte výchozí konfiguraci zabezpečení.
4. Zapněte vlastní konfiguraci zabezpečení v souboru `mqwebuser.xml` a uveďte certifikát, který chcete prezentovat.

Procedura předpokládá, že jste:

- Použití systému AIX, Linux, and Windows .
- Oprávněný uživatel.

Notes:

- Následující příklad vytvoří a použije certifikát podepsaný svým držitelem pomocí příkazů vydaných na počítači se systémem Linux , tj. **ls**, spíše než **dir** použitých na počítači se systémem Windows .
- Zobrazí se koncept, ale neodebere varování prohlížeče.
- Chcete-li odebrat varování prohlížeče, musíte poskytnout certifikát podepsaný certifikační autoritou.

Postup

1. Pokud je server Liberty spuštěn, zastavte jej zadáním příkazu **endmqweb** na příkazovém řádku.
2. Přidejte certifikát do úložiště klíčů, které používá aplikační server Liberty , aby mohl najít a prezentovat certifikát ve webovém prohlížeči.
   a) Přejděte do umístění úložiště klíčů zadáním následujícího příkazu a vypište výstup:

```
cd /var/mqm/web/installations/Installation1/servers/mqweb/resources/security
ls
```

Například uvidíte následující výstup, který zobrazí úložiště klíčů s názvem `key.jks`:

```
/var/mqm/web/installations/Installation1/servers/mqweb/resources/security$
ls key.jks ltpa.keys
```

b) Vytvořte certifikát podepsaný svým držitelem:

Chcete-li vytvořit certifikát podepsaný svým držitelem pro vzdělávací účely, který se přidá do `key.jks` s heslem `password`, zadejte následující příkaz:

```
runmqckm -cert -create -db key.jks -pw password -dn
"cn=QueueManager,o=IBM,c=UK" -label myowncertificate
```

Příznak **-dn** vám umožňuje uvést hodnoty zobrazené na vašem certifikátu.

c) Zadáním následujícího příkazu ověřte, že jste úspěšně přidali certifikát:

```
runmqckm -cert -list -db key.jks -pw password
```

Například uvidíte následující výstup, který ukazuje, že certifikát byl přidán s jeho popiskem, spolu s certifikátem označeným `default` , který server momentálně používá:

```
/var/mqm/web/installations/Installation1/servers/mqweb/resources/security
$ runmqckm -cert -list -db key.jks -pw password
Certificates in database /var/mqm/web/installations/Installation1/servers/mqweb/resources/
security/key.jks
   default
   myown certificate
```

3. Upravte soubor `mqwebuser.xml` tak, aby server poskytoval nový certifikát.

a) Přesuňte se do umístění souboru `mqwebuser.xml` a poté jej otevřete pro úpravy v textovém editoru dle vašeho výběru, v tomto případě *nano* .

```
cd /var/mqm/web/installations/Installation1/servers/mqweb
nano mqwebuser.xml
```

b) Vypněte výchozí konfiguraci zabezpečení.

Označte následující řádek jako komentář přidáním řetězce `<!--` na začátek řádku kódu a řetězce `-->` na konec řádku kódu:

```
<!--
<sslDefault sslRef="mqDefaultSSLConfig"/>
-->
```

c) Povolte a určete vlastní konfiguraci.

Chcete-li to provést, proveďte následující postup:

i) Zrušte komentář u následujících řádků kódu tak, že odeberete znak `<!--` ze začátku bloku kódu a znak `-->` z konce bloku kódu.

```
<!--
<keyStore id="defaultKeyStore" location="key.jks" type="JKS" password="password"/>
<keyStore id="defaultTrustStore" location="trust.jks" type="JKS" password="password"/>
<ssl id="thisSSLConfig" clientAuthenticationSupported="true" keyStoreRef="defaultKeyStore"
serverKeyAlias="default" trustStoreRef="defaultTrustStore" sslProtocol="TLSv1.2"/>
<sslDefault sslRef="thisSSLConfig"/>
-->
```

ii) **Neměňte první řádek** bloku kódu, protože tento řádek určuje úložiště klíčů, které konzola používá k uložení svých osobních certifikátů.

iii) **Označte jako komentář druhý řádek bloku kódu**, protože tento řádek uvádí úložiště údajů o důvěryhodnosti, kde by konzola hledala certifikáty klienta. Protože používáte ověření tokenu, nevytvořili jste úložiště údajů o důvěryhodnosti a ponechání řádku kódu by způsobilo chybu při spuštění konzoly.

iv) **Změnit serverKeyAlias= "default" na serverKeyAlias= "myowncertificate"** ve třetím řádku bloku kódu a nechat vše ostatní stejné.

v) **Neměňte poslední řádek** bloku kódu, protože to říká serveru, aby používal konfiguraci, kterou jste právě uvedli.

Blok kódu nyní vypadá takto:

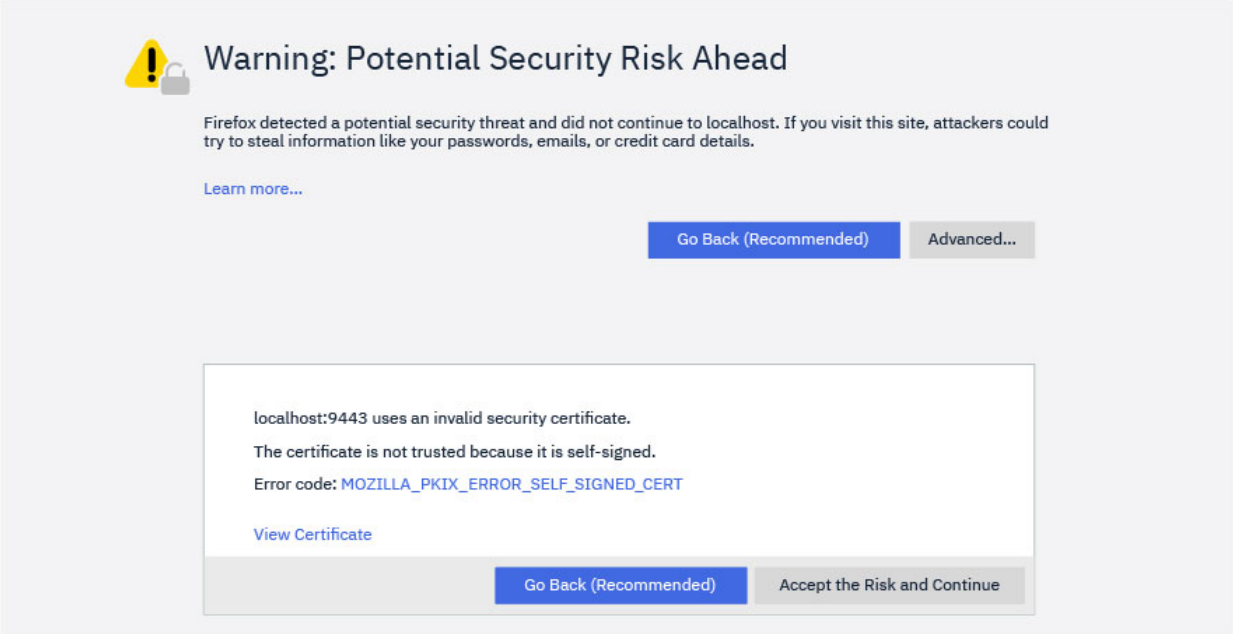
```
<keyStore id="defaultKeyStore" location="key.jks" type="JKS" password="password"/>
<!-- Commenting out the defaultTrustStore as otherwise we get errors (viewable in the messages.log file
in the logs folder) j
<keyStore id="defaultTrustStore" location="trust.jks" type="JKS" password="password"/>
-->
<ssl id="thisSSLConfig" clientAuthenticationSupported="true" keyStoreRef="defaultKeyStore"
serverKeyAlias="myowncertificate" trustStoreRef="defaultTrustStore" sslProtocol="TLSv1.2"/>
<sslDefault sslRef="thisSSLConfig"/>
```

4. Restartujte webový server pomocí příkazu **strmqweb** .

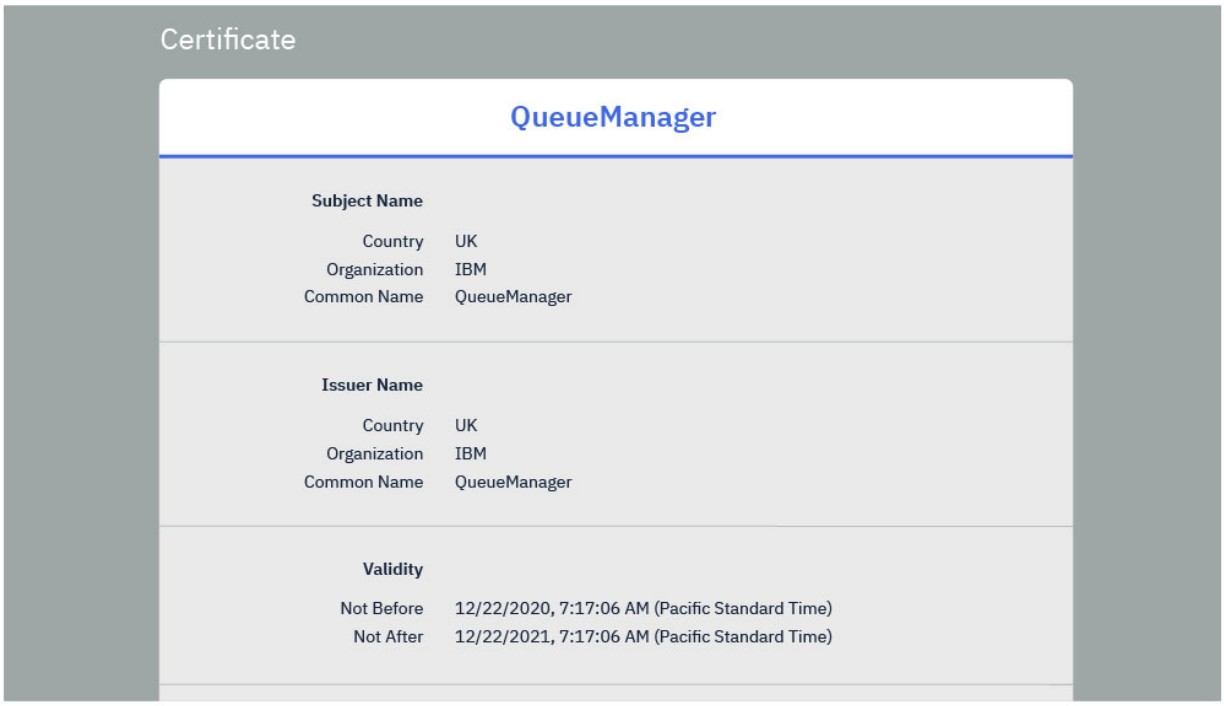
Výsledky

Po spuštění webového serveru vyhledejte soubor IBM MQ Console a proveďte jeho aktualizaci.
Pokud používáte certifikát podepsaný (svým) držitelem, který jste vytvořili, pomocí postupu popsaného v předchozím textu v krocích “2” na stránce 539 a “3” na stránce 540, zobrazí se varování zabezpečení.

Všimněte si, že formát tohoto varování závisí na používaném prohlížeči.



Klepnete-li na volbu **Zobrazit certifikát**, uvidíte, že obsahuje podrobnosti, které jste zadali v příznaku **-dn** při vytváření certifikátu v kroku “2.b” na stránce 540.



Pokud však používáte certifikát podepsaný certifikační autoritou, váš prohlížeč důvěřuje, což jste přidali zadáním následujícího příkazu:

```
runmqckm -cert -add -db key.jks -pw password -label myCACertificate
```

kde `myCACertificate` je cesta k souboru s vaším certifikátem CA, který se dostanete přímo na přihlašovací stránku.

Upozornění: Používáte-li certifikát podepsaný certifikační autoritou a tento certifikát certifikační autority je součástí řetězu certifikátů, musíte do řetězu přidat všechny certifikáty počínaje kořenovým certifikátem certifikační autority. Další informace viz “Přidání certifikátu CA nebo veřejné části certifikátu podepsaného držitelem do úložiště klíčů v systému AIX, Linux, and Windows” na stránce 318.

ALW Použití ověření pomocí certifikátu klienta s REST API a IBM MQ Console

Certifikáty klienta můžete mapovat na činitele pro ověření uživatelů IBM MQ Console a REST API .

Než začnete

- Nakonfigurujte uživatele, skupiny a role, aby byly autorizovány pro použití IBM MQ Console a REST API. Další informace viz téma “Konfigurace uživatelů a rolí” na stránce 527.
- Když použijete REST API, můžete se dotázat na pověření aktuálního uživatele pomocí metody HTTP GET na prostředku `login` a poskytnout certifikát klienta pro ověření požadavku. Tento požadavek vrací informace o jménu uživatele a rolích, které jsou uživateli přiřazeny. Další informace viz GET `/login`.
- Když mapujete certifikáty klienta na činitele pro ověření uživatelů, rozlišující název certifikátu klienta se použije pro porovnání s uživateli v konfigurovaném registru uživatelů:
  - V případě základního registru se obecný název (CN) porovnává s uživatelem. Například `CN=Fred, O=IBM, C=GB` se shoduje se jménem uživatele `Fred`.

– Pro registr LDAP se standardně porovnává úplný rozlišující název s LDAP. Můžete nastavit filtry a mapování pro přizpůsobení shody. Další informace viz Režim mapování certifikátů Liberty :LDAP v dokumentaci WebSphere Liberty .

Informace o této úloze

Když se uživatel ověřuje pomocí certifikátu klienta, použije se certifikát místo jména uživatele a hesla. Pro produkt REST APIje certifikát klienta poskytnut s každým požadavkem REST pro ověření uživatele. Pro server IBM MQ Consoleplatí, že když se uživatel přihlásí pomocí certifikátu, nemůže být poté odhlášen.

Procedura předpokládá následující informace:

- Váš soubor `mqwebuser.xml` je založen na jedné z následujících ukázek:
  - `basic_registry.xml`
  - `local_os_registry.xml`
  - `ldap_registry.xml`
- Že používáte systém AIX, Linux, and Windows .
- Jste privilegovaný uživatel.

Chcete-li nakonfigurovat ověření klientských certifikátů pomocí RACF svazku klíčů na systému z/OS, postupujte podle pokynů v části “Konfigurace TLS pro REST API a IBM MQ Console na z/OS” na stránce 555.

Poznámka: Následující procedura popisuje kroky nezbytné pro použití certifikátů klienta s IBM MQ Console a REST API. Pro usnadnění práce vývojáře jsou uvedeny podrobné informace o tom, jak vytvářet a používat certifikáty podepsané svým držitelem. Pro výrobu však použijte certifikáty, které byly získány od certifikační autority.

Postup

1. Spusťte server mqweb zadáním příkazu **strmqweb** na příkazovém řádku.
2. Vytvořte certifikát klienta:
   a) Vytvořte úložiště klíčů PKCS#12 :
      i) Otevřete nástroj správy klíčů IBM zadáním příkazu **strmqikm** na příkazovém řádku.
      ii) V nabídce **Soubor databáze klíčů** v nástroji správy klíčů IBM klepněte na volbu **Nový**.
      iii) Ze seznamu **Typ databáze klíčů** vyberte **PKCS12** .
      iv) Vyberte umístění pro uložení úložiště klíčů a zadejte odpovídající název do pole **Název souboru** . Například `user.p12`
      v) Po zobrazení výzvy nastavte heslo.
   b) Vytvořte certifikát, buď vytvořením certifikátu podepsaného svým držitelem, nebo získáním certifikátu od certifikační autority:
      - Vytvořte certifikát podepsaný svým držitelem:
        i) Klepněte na volbu **Nový podpis sám sebou**.
        ii) Zadejte `user` do pole **Popisek klíče** .
        iii) Používáte-li základní registr uživatelů, zadejte jméno uživatele ze svého registru uživatelů do pole **Obecný název** . Například `mqadmin`. V případě registru uživatelů LDAP se ujistěte, že rozlišující název certifikátu odpovídá rozlišujícímu názvu v registru LDAP.
        iv) Klepněte na tlačítko **OK**.
      - Získejte certifikát od certifikační autority. Certifikát CA musí obsahovat příslušné jméno uživatele v rámci obecného názvu (CN) pole rozlišujícího názvu (DN):
        i) Vyžádejte si nový certifikát. V nabídce **Vytvořit** klepněte na volbu **Nová žádost o certifikát**.
        ii) Do pole **Popisek klíče** zadejte popisek certifikátu.

iii) Používáte-li základní registr uživatelů, zadejte do pole **Obecný název** jméno uživatele, pro kterého je certifikát určen.

Pokud používáte lokální registr OS, pole **Obecný název** se musí shodovat s ID uživatele lokálního operačního systému.

V případě registru uživatelů LDAP se ujistěte, že rozlišující název certifikátu odpovídá rozlišujícímu názvu v registru LDAP.

iv) Zadejte nebo vyberte hodnoty pro zbývající pole, podle potřeby.

v) Vyberte umístění pro uložení žádosti o certifikát a název souboru pro žádost o certifikát a klepněte na tlačítko **OK**.

vi) Odešlete soubor žádosti o certifikát certifikační autoritě (CA).

vii) Máte-li certifikát od CA, otevřete nástroj pro správu klíčů IBM zadáním příkazu **strmqikm** na příkazovém řádku.

viii) V nabídce **Soubor databáze klíčů** v nástroji správy klíčů IBM klepněte na volbu **Otevřít**.

ix) Vyberte úložiště klíčů PKCS#12 , které obsahuje certifikát klienta. Například: `user.p12`

x) Klepněte na tlačítko **Přijmout**, vyberte příslušný certifikát a klepněte na tlačítko **OK**.

3. Extrahujte veřejnou část certifikátu klienta:
   a) Otevřete nástroj správy klíčů IBM zadáním příkazu **strmqikm** na příkazovém řádku.
   b) V nabídce **Soubor databáze klíčů** v nástroji správy klíčů IBM klepněte na volbu **Otevřít**.
   c) Vyberte úložiště klíčů PKCS#12 , které obsahuje certifikát klienta. Například: `user.p12`
   d) Vyberte certifikát klienta ze seznamu certifikátů v nástroji Správa klíčů IBM .
   e) Klepněte na volbu **Extrahovat certifikát**.
   f) Vyberte umístění pro uložení certifikátu a zadejte odpovídající název souboru do pole **Název souboru certifikátu** . Například `user.arm`.
4. Importujte veřejnou část certifikátu klienta do úložiště klíčů důvěryhodnosti serveru mqweb jako certifikát podepsaného, aby mohl server ověřit certifikát klienta:
   a) Vytvořte úložiště klíčů `trust.jks` pro použití serverem mqweb, pokud dosud neexistuje:
      i) V nabídce **Soubor databáze klíčů** v nástroji správy klíčů IBM klepněte na volbu **Nový**.
      ii) Vyberte volbu **JKS** ze seznamu **Typ databáze klíčů** .
      iii) Klepněte na tlačítko **Procházet** a přejděte na: `MQ_DATA_DIRECTORY/web/installations/installationName/servers/mqweb/resources/security`.

      Tento adresář by již měl obsahovat soubor `key.jks` . Pokud soubor `trust.jks` již existuje, otevřete jej a nepřepisujete jej.

      iv) Zadejte `trust.jks` do pole **Název souboru** .
      v) Po zobrazení výzvy nastavte heslo.
   b) V rozevírací nabídce vyberte volbu **Certifikáty podepsaného**.
   c) Klepněte na tlačítko **Přidat**.
   d) Vyberte příslušný soubor raménka a klepněte na tlačítko **OK**. Vyberte například `user.arm`.
   e) Zadejte popisek pro certifikát.
5. Změňte heslo úložiště klíčů serveru mqweb:
   a) V nabídce **Soubor databáze klíčů** klepněte na volbu **Otevřít**.
   b) Vyberte volbu **JKS** ze seznamu **Typ databáze klíčů** .
   c) Klepněte na tlačítko **Procházet** a přejděte na *MQ_DATA_PATH*`/web/installations/`*installationName*`/servers/mqweb/resources/security` .
   d) Vyberte úložiště klíčů `key.jks` a klepněte na tlačítko **Otevřít**.
   e) Po zobrazení výzvy zadejte heslo. Výchozí heslo je `password`.

f) V nabídce **Soubor databáze klíčů** klepněte na volbu **Změnit heslo**.

g) Zadejte nové heslo pro úložiště klíčů.

6. Povolte ověření klientských certifikátů v souboru `mqwebuser.xml` :

   Soubor `mqwebuser.xml` lze nalézt na následující cestě: *MQ_DATA_PATH*`/web/installations/`*installationName*`/servers/mqweb`

   a) Zrušte komentář u sekce v souboru `mqwebuser.xml` , která umožňuje ověření klientských certifikátů. Sekce obsahuje následující text:

   ```
   <keyStore id="defaultKeyStore" location="key.jks" type="JKS" password="password"/>
       <keyStore id="defaultTrustStore" location="trust.jks" type="JKS" password="password"/>
       <ssl id="thisSSLConfig" clientAuthenticationSupported="true"
   keyStoreRef="defaultKeyStore"
               trustStoreRef="defaultTrustStore" sslProtocol="TLSv1.2"
   serverKeyAlias="default"/>
       <sslDefault sslRef="thisSSLConfig"/>
   ```

   b) Zkontrolujte, zda hodnota **serverKeyAlias** odpovídá názvu certifikátu serveru. Pokud používáte výchozí certifikát serveru, hodnota je správná.

   c) Změňte hodnotu **password** pro `defaultKeyStore` na zakódovanou verzi hesla pro úložiště klíčů `key.jks` :

      i) V adresáři *MQ_INSTALLATION_PATH*`/web/bin` zadejte na příkazový řádek následující příkaz:

      ```
      securityUtility encode password
      ```

      ii) Umístěte výstup tohoto příkazu do pole **heslo** pro `defaultKeyStore`.

   d) Změňte hodnotu pro **heslo** pro `defaultTrustStore` tak, aby odpovídala heslu pro úložiště klíčů `trust.jks` :

      i) V adresáři *MQ_INSTALLATION_PATH*`/web/bin` zadejte na příkazový řádek následující příkaz:

      ```
      securityUtility encode password
      ```

      ii) Umístěte výstup tohoto příkazu do pole **heslo** pro `defaultTrustStore`.

   e) Odeberte nebo označte jako komentář následující řádek ze souboru `mqwebuser.xml` :

   ```
   <sslDefault sslRef="mqDefaultSSLConfig"/>
   ```

7. Zastavte server mqweb zadáním příkazu **endmqweb** na příkazovém řádku.
8. Spusťte server mqweb zadáním příkazu **strmqweb** na příkazovém řádku.
9. Použít certifikát klienta k ověření:

   - Chcete-li použít certifikát klienta s produktem IBM MQ Console, nainstalujte certifikát klienta do webového prohlížeče, který se používá pro přístup k serveru IBM MQ Console. Například nainstalujte certifikát klienta `user.p12` jako osobní certifikát.
   - Chcete-li použít certifikát klienta s produktem REST API, poskytněte certifikát klienta s každým požadavkem REST. Používáte-li metody HTTP POST, PATCH nebo DELETE, musíte poskytnout další ověření s certifikátem klienta, abyste zabránili útokům typu padělání požadavků mezi servery. To znamená, že další ověření se používá k potvrzení, že pověření, která se používají k ověření požadavku, jsou používána vlastníkem pověření.

     Toto dodatečné ověření poskytuje záhlaví `ibm-mq-rest-csrf-token` HTTP . Nastavte hodnotu záhlaví `ibm-mq-csrf-token` na cokoli včetně mezery, pak odešlete požadavek.

Příklad

Důležité: V tomto příkladu ne všechny implementace cURL podporují certifikáty podepsané sebou samým, takže musíte použít implementaci cURL , která tak činí.

Následující příklad cURL ukazuje, jak vytvořit novou frontu Q1ve správci front QM1s ověřením pomocí certifikátu klienta. Přesná konfigurace tohoto příkazu cURL závisí na knihovnách, na kterých byla sestavena cURL . Příklad je založen na systému Windows , s adresou cURL sestavenou pro OpenSSL.

- Použijte metodu HTTP POST s prostředkem fronty, ověřením pomocí certifikátu klienta a včetně záhlaví `ibm-mq-rest-csrf-token` HTTP s libovolnou hodnotou. Tato hodnota může být libovolná, včetně prázdné hodnoty. Příznak `--cert-type` určuje, že certifikát je certifikátem PKCS#12 . Příznak `--cert` uvádí umístění certifikátu, následovaný dvojtečkou,:, a pak heslo pro certifikát:

```
curl -k https://localhost:9443/ibmmq/rest/v1/admin/qmgr/QM1/queue -X POST -
-cert-type P12 --cert c:\user.p12:password
-H "ibm-mq-rest-csrf-token: value"
-H "Content-Type: application/json" --data "{\"name\":\"Q1\"}"
```

Použití základního ověření HTTP s REST API

Uživatelé produktu REST API se mohou ověřit zadáním ID uživatele a hesla v záhlaví HTTP . Chcete-li použít tuto metodu ověření s metodami HTTP , jako např. POST, PATCH a DELETE, musí být také poskytnuto záhlaví `ibm-mq-rest-csrf-token` HTTP , stejně jako ID uživatele a heslo.

Než začnete

- Nakonfigurujte uživatele, skupiny a role, které mají být autorizovány k použití produktu REST API. Další informace viz téma “Konfigurace uživatelů a rolí” na stránce 527.
- Ujistěte se, že je povoleno základní ověření HTTP . Zkontrolujte, zda je v souboru `mqwebuser.xml` přítomen následující kód XML, který není označen jako komentář. Tento kód XML musí být v rámci značek `<featureManager>` :

```
<feature>basicAuthenticationMQ-1.0</feature>
```

z/OS V systému z/OSmusíte být uživatelem, který má přístup pro zápis do souboru `mqwebuser.xml` , abyste mohli tento soubor upravit.

Multi Na všech ostatních operačních systémech musíte být privilegovaný uživatel , abyste mohli upravovat soubor `mqwebuser.xml` .

- Při odesílání požadavků REST se ujistěte, že používáte zabezpečené připojení. Protože kombinace jména uživatele a hesla jsou kódovány, ale nejsou šifrovány, musíte použít zabezpečené připojení (HTTPS), když používáte základní ověření HTTP s produktem REST API.
- Můžete se dotázat na pověření aktuálního uživatele pomocí metody HTTP GET na prostředku `login` , která poskytuje základní ověřovací informace pro ověření požadavku. Tento požadavek vrací informace o jménu uživatele a rolích, které jsou uživateli přiřazeny. Další informace viz GET `/login`.

Postup

1. Jméno uživatele zřetězte dvojtečkou a heslem. Všimněte si, že jméno uživatele rozlišuje velikost písmen.

   Například jméno uživatele admin a heslo admin se stane následujícím řetězcem:

   ```
   admin:admin
   ```

2. Zakódujte tento řetězec jména uživatele a hesla v kódování base64 .
3. Toto zakódované jméno uživatele a heslo zahrňte do záhlaví HTTP `Authorization: Basic` .

   Například s zakódovaným jménem uživatele admin a heslem admin se vytvoří následující záhlaví:

   ```
   Authorization: Basic YWRtaW46YWRtaW4=
   ```

4. Používáte-li metody HTTP POST, PATCH nebo DELETE, musíte poskytnout další ověření a také jméno uživatele a heslo.

Toto dodatečné ověření poskytuje záhlaví `ibm-mq-rest-csrf-token` HTTP . Záhlaví `ibm-mq-rest-csrf-token` HTTP musí být přítomno v požadavku, ale jeho hodnota může být libovolná, včetně prázdné hodnoty.

5. Odešlete požadavek REST do produktu IBM MQ s příslušnými záhlavími.

Příklad

Následující příklad ukazuje, jak vytvořit novou frontu `Q1`ve správci front `QM1`se základním ověřením v systémech Windows . Příklad používá cURL:

- Použijte metodu HTTP POST s prostředkem fronty, ověření se základním ověřením a včetně záhlaví `ibm-mq-rest-csrf-token` HTTP s libovolnou hodnotou. Tato hodnota může být libovolná, včetně prázdné hodnoty:

```
curl -k https://localhost:9443/ibmmq/rest/v1/admin/qmgr/QM1/queue -X POST
-u mqadmin:mqadmin
-H "ibm-mq-rest-csrf-token: value"
-H "Content-Type: application/json" --data "{\"name\":\"Q1\"}"
```

Použití ověření založeného na tokenech s rozhraním REST API

Uživatelé produktu REST API se mohou ověřit zadáním ID uživatele a hesla do prostředku produktu REST API `login` pomocí metody HTTP POST. Je vygenerován token LTPA, který umožňuje uživateli ověřit budoucí požadavky. Tento token LTPA má předponu `LtpaToken2`. Uživatel se může odhlásit pomocí metody HTTP DELETE a může se dotazovat na přihlašovací informace aktuálního uživatele pomocí metody HTTP GET.

Než začnete

- Nakonfigurujte uživatele, skupiny a role, které mají být autorizovány k použití produktu REST API. Další informace viz téma “Konfigurace uživatelů a rolí” na stránce 527.
- Standardně název souboru cookie, který obsahuje token LTPA, začíná řetězcem `LtpaToken2`a obsahuje příponu, kterou lze změnit při restartování serveru mqweb. Tento náhodný název souboru cookie umožňuje spuštění více než jednoho serveru mqweb na stejném systému. Pokud však chcete, aby název souboru cookie zůstal konzistentní hodnotou, můžete zadat název, který má soubor cookie, pomocí příkazu **setmqweb** . Další informace viz Konfigurace tokenu LTPA.
- Standardně vyprší platnost souboru cookie tokenu LTPA po 120 minutách. Čas vypršení platnosti souboru cookie tokenu LTPA můžete nakonfigurovat pomocí příkazu **setmqweb** . Další informace viz Konfigurace tokenu LTPA.
- Při odesílání požadavků REST se ujistěte, že používáte zabezpečené připojení. Když použijete metodu HTTP POST na prostředku `login` , kombinace jména uživatele a hesla, která se odešle s požadavkem, se nezašifruje. Proto musíte použít zabezpečené připojení (HTTPS), když používáte ověření založené na tokenech s produktem REST API. Standardně nemůžete použít HTTP s ověřením tokenu LTPA. Token LTPA, který má být používán nezabezpečenými HTTP připojeními, můžete povolit nastavením parametru **secureLTPA** na hodnotu `False`. Další informace viz Konfigurace tokenu LTPA.
- Můžete se dotázat na pověření aktuálního uživatele pomocí metody HTTP GET na prostředku `login` , která poskytuje token LTPA pro ověření požadavku. Tento požadavek vrací informace o jménu uživatele a rolích, které jsou uživateli přiřazeny. Další informace viz GET `/login`.

Postup

1. Přihlaste se k uživateli:
   a) Použijte metodu HTTP POST na prostředku `login` :

   ```
   https://host:port/ibmmq/rest/v1/login
   ```

   Do těla požadavku JSON zahrňte jméno uživatele a heslo v následujícím formátu:

```
{
    "username" : name,
    "password" : password
}
```

b) Uložte token LTPA, který je vrácen z požadavku, do lokálního úložiště souborů cookie. Standardně má tento token LTPA předponu `LtpaToken2`.

2. Ověřit požadavky REST s uloženým tokenem LTPA jako soubor cookie s každým požadavkem.

   Pro požadavky, které používají metody HTTP PUT, PATCH nebo DELETE, uveďte záhlaví `ibm-mq-rest-csrf-token` . Hodnota tohoto záhlaví může být libovolná, včetně prázdné hodnoty.

3. Odhlásit uživatele:

   a) Použijte metodu HTTP DELETE na prostředku `login` :

   ```
   https://host:9443/ibmmq/rest/v1/login
   ```

   Musíte poskytnout token LTPA jako soubor cookie pro ověření požadavku a zahrnout záhlaví `ibm-mq-rest-csrf-token` . Hodnota tohoto záhlaví může být cokoli, včetně prázdné hodnoty.

   b) Zpracujte pokyny k odstranění tokenu LTPA z lokálního úložiště souborů cookie.

   Poznámka: Pokud instrukce není zpracována a token LTPA zůstane v lokálním úložišti souborů cookie, lze token LTPA použít k ověření budoucích požadavků REST. To znamená, že když se uživatel pokusí ověřit pomocí tokenu LTPA po ukončení relace, vytvoří se nová relace, která použije existující token.

Příklad

Následující příklad cURL ukazuje, jak vytvořit novou frontu `Q1`ve správci front `QM1`s ověřením založeným na tokenech v systémech Windows :

- Přihlaste se a přidejte token LTPA s předponou `LtpaToken2`do lokálního úložiště souborů cookie. Informace o jménu uživatele a hesle jsou zahrnuty v těle JSON. Příznak `-c` určuje umístění souboru, do kterého má být token uložen:

  ```
  curl -k https://localhost:9443/ibmmq/rest/v1/login -X POST
  -H "Content-Type: application/json" --data
  "{\"username\":\"mqadmin\",\"password\":\"mqadmin\"}"
  -c c:\cookiejar.txt
  ```

- Vytvořte frontu. Použijte metodu HTTP POST s prostředkem fronty, která se ověřuje s tokenem LTPA. Token LTPA s předponou `LtpaToken2` je načten ze souboru `cookiejar.txt` pomocí příznaku `-b` . Ochrana CSRF je poskytována přítomností záhlaví `ibm-mq-rest-csrf-token` HTTP :

  ```
  curl -k https://localhost:9443/ibmmq/rest/v1/admin/qmgr/QM1/queue -X POST -b
  c:\cookiejar.txt -H "ibm-mq-rest-csrf-token: value" -H "Content-Type: application/json"
  --data "{\"name\":\"Q1\"}"
  ```

- Odhlaste se a odstraňte token LTPA z lokálního úložiště souborů cookie. Token LTPA je načten ze souboru `cookiejar.txt` pomocí příznaku `-b` . Ochrana CSRF je poskytována přítomností záhlaví `ibm-mq-rest-csrf-token` HTTP . Umístění souboru `cookiejar.txt` je určeno příznakem `-c` , takže token LTPA je odstraněn ze souboru:

  ```
  curl -k https://localhost:9443/ibmmq/rest/v1/admin/qmgr/QM1/queue -X DELETE
  -H "ibm-mq-rest-csrf-token: value" -b c:\cookiejar.txt
  -c c:\cookiejar.txt
  ```

Související odkazy

POST /login

GET /login

ODSTRANIT /login

Vložení IBM MQ Console do sekce IFrame

Prvek HTML < iframe> lze použít k vložení jedné webové stránky do jiné pomocí vloženého rámce (IFrame). Z bezpečnostních důvodů nelze IBM MQ Console standardně vložit do názvu IFrame. Název IFrame však můžete povolit pomocí vlastnosti konfigurace **mqConsoleFrameAncestors** na serveru mqweb.

Informace o této úloze

Server mqweb udržuje seznam povolených původů webových stránek, které mohou vložit soubor IBM MQ Console pomocí názvu IFrame. Původ je kombinací schématu URL , domény a portu, například `https://example.com:1234`.

K určení položek v seznamu můžete použít vlastnost konfigurace **mqConsoleFrameAncestors** na serveru mqweb.

Standardně je hodnota **mqConsoleFrameAncestors** prázdná, což znamená, že IBM MQ Console nelze vložit do názvu IFrame.

Postup

Zadejte seznam původů webových stránek, které mohou vložit IBM MQ Console do názvu IFrame, zadáním následujícího příkazu:

```
setmqweb properties -k mqConsoleFrameAncestors -v allowedOrigins
```

kde *allowedOrigins* je seznam původů oddělených čárkami. Každý původ by se měl skládat z:

- Název hostitele nebo adresa IP
- Volitelné schéma URL
- Volitelné číslo portu

Všimněte si, že název hostitele může začínat zástupným znakem (*) a číslo portu může také používat zástupný znak (*).

Příklady původu jsou:

```
https://example.com:1234
```

který umožňuje jakékoli webové stránce obsluhované z produktu `https://example.com:1234` vložit IBM MQ Console do IFrame.

```
https://*.example.com:*
```

který umožňuje jakékoli webové stránce HTTPS s názvem hostitele končícím na `example.com`a pomocí libovolného portu vložit IBM MQ Console do názvu IFrame.

Příklad

Následující příklad umožňuje, aby byl soubor IBM MQ Console vložen do názvu IFrame z webových stránek obsluhovaných z produktu `https://site2.example.com:1234` nebo `https://site2.example.com:1235`:

```
setmqweb properties -k mqConsoleFrameAncestors -v
https://site2.example.com:1234,https://site2.example.com:1235
```

Konfigurace CORS pro REST API

Standardně webový prohlížeč nedovoluje skriptům, jako je JavaScript, vyvolat skript REST API , když není ze stejného původu jako skript REST API. To znamená, že požadavky na křížový původ nejsou povoleny.

Můžete konfigurovat sdílení CORS (Cross Origin Resource Sharing), abyste povolili požadavky na křížový původ od určeného původu.

Informace o této úloze

K produktu REST API můžete přistupovat prostřednictvím webového prohlížeče, například prostřednictvím skriptu. Vzhledem k tomu, že tyto požadavky jsou z jiného původu než požadavky REST API, webový prohlížeč požadavek odmítne, protože se jedná o požadavek z jiného původu. Původ se liší, pokud doména, port nebo schéma nejsou stejné.

Máte-li například skript, který je hostován na adrese `http://localhost:1999/` , provedete požadavek na křížový původ, pokud zadáte příkaz HTTP GET na webovém serveru, který je hostován na adrese `https://localhost:9443/`. Tento požadavek je požadavek křížového původu, protože čísla portů a schéma (HTTP) se liší.

Požadavky různých původů můžete povolit konfigurací CORS a určením původů, které mají povolen přístup k produktu REST API.

Další informace o CORS viz https://www.w3.org/TR/cors/ a https://developer.mozilla.org/en-US/docs/Web/HTTP/CORS.

Postup

1. Zobrazte aktuální konfiguraci zadáním následujícího příkazu:

   ```
   dspmqweb properties -a
   ```

   Položka `mqRestCorsAllowedOrigins` uvádí povolený původ. Položka `mqRestCorsMaxAgeInSeconds` určuje dobu v sekundách, po kterou může webový prohlížeč ukládat výsledky všech předletových kontrol CORS do mezipaměti.
2. Zadejte původy, které mají povolen přístup k serveru REST API , zadáním následujícího příkazu:

   ```
   setmqweb properties -k mqRestCorsAllowedOrigins -v allowedOrigins
   ```

   kde *allowedOrigins* uvádí původ, ze kterého chcete povolit požadavky na křížový původ. Chcete-li povolit všechny požadavky křížového původu, můžete použít hvězdičku uzavřenou do dvojitých uvozovek "*". Můžete zadat více než jeden původ v seznamu odděleném čárkami, uzavřený do dvojitých uvozovek. Chcete-li povolit žádné požadavky na křížový původ, zadejte prázdné uvozovky jako hodnotu pro *allowedOrigins*.
3. Zadejte dobu v sekundách, po kterou chcete webovému prohlížeči povolit ukládání výsledků předletových kontrol CORS do mezipaměti, zadáním následujícího příkazu:

   ```
   setmqweb properties -k mqRestCorsMaxAgeInSeconds -v time
   ```

Příklad

Následující příklad zobrazuje požadavky různých původů povolené pro `http://localhost:9883`, `https://localhost:1999`a `https://localhost:9663`. Maximální stáří výsledků předletových kontrol CORS uložených v mezipaměti je nastaveno na 90 sekund:

```
setmqweb properties -k mqRestCorsAllowedOrigins -v "http://localhost:9883,https://
localhost:1999,https://localhost:9663"
setmqweb properties -k mqRestCorsMaxAgeInSeconds -v 90
```

Konfigurace ověření záhlaví hostitele pro IBM MQ Console a REST API

Server mqweb můžete nakonfigurovat tak, aby omezil přístup k IBM MQ Console a REST API tak, aby byly zpracovány pouze požadavky odeslané se záhlavím hostitele, které odpovídá zadanému seznamu povolení. Pokud je použita hodnota záhlaví hostitele, která není v seznamu povolených, je vrácena chyba.

Informace o této úloze

Server mqweb používá k definování seznamu povolených přijatelných záhlaví hostitele virtuální hostitele. Další informace o virtuálních hostitelích naleznete v dokumentaci k produktu WebSphere Liberty : https://www.ibm.com/docs/SSEQTP_liberty/com.ibm.websphere.wlp.doc/ae/cwlp_virtual_hosts.html

Chcete-li dokončit tuto úlohu, musíte být uživatel s dostatečnými oprávněními k úpravě souboru `mqwebuser.xml` :

- z/OS V systému z/OSmusíte mít přístup pro zápis do souboru `mqwebuser.xml` .
- Multi U všech ostatních operačních systémů musíte být privilegovaný uživatel.
- V 9.3.5 Linux Pokud je server mqweb součástí samostatné instalace produktu IBM MQ Web Server , musíte mít přístup pro zápis k souboru `mqwebuser.xml` v datovém adresáři IBM MQ Web Server .

Postup

1. Otevřete soubor `mqwebuser.xml` . Tento soubor se nachází v jednom z následujících umístění:
   - V instalaci produktu IBM MQ :
     - Linux AIX V systému AIX nebo Linux: `/var/mqm/web/installations/`*`installationName`*`/servers/mqweb`
     - Windows V systému Windows: *MQ_DATA_PATH*`\web\installations\`*`installationName`*`\servers\mqweb`, kde *MQ_DATA_PATH* je cesta k datům IBM MQ . Tato cesta je cestou k datům, která je vybrána během instalace produktu IBM MQ. Standardně je tato cesta `C:\ProgramData\IBM\MQ`.
     - z/OS V systému z/OS: *WLP_user_directory*`/servers/mqweb`

       Kde *WLP_user_directory* je adresář, který byl zadán při spuštění příkazu **crtmqweb** pro vytvoření definice serveru mqweb.
   - V 9.3.5 Linux V samostatné IBM MQ Web Server instalaci: *MQ_OVERRIDE_DATA_PATH*`/web/installations/MQWEBINST/servers/mqweb`

     kde *MQ_OVERRIDE_DATA_PATH* je datový adresář IBM MQ Web Server , na který odkazuje proměnná prostředí **MQ_OVERRIDE_DATA_PATH** .
2. Přidejte nebo zrušte komentář u následujícího kódu v souboru `mqwebuser.xml` :

```
<virtualHost allowFromEndpointRef="defaultHttpEndpoint" id="default_host">
        <hostAlias>localhost:9080</hostAlias>
</virtualHost>
```

3. Upravte pole **<hostAlias>** vložením kombinace názvu hostitele a portu, které chcete povolit.

   Tato kombinace může být názvem hostitele a názvem portu, který jste použili v konfiguraci serveru mqweb. Pokud například použijete výchozí konfiguraci `localhost:9443`, můžete použít `localhost:9443` v poli **<hostAlias>** .

   V případě potřeby můžete do značek **<virtualHost>** přidat více polí **<hostAlias>** , abyste umožnili více kombinací názvu hostitele a portu. Chcete-li například povolit záhlaví hostitele, která používají port HTTP , a také záhlaví hostitele, která používají port HTTPS .

Auditování

Záznamy auditu operací prováděných v systémech IBM MQ Console a REST API lze vytvořit povolením příkazů a konfiguračních událostí správce front a v systému AIX, Linux, and Windows se do souborů protokolu serveru mqweb zaznamenávají významné změny stavu.

Významné změny stavu

ALW

V systému AIX, Linux, and Windowsprodukt IBM MQ Console zaznamenává významné změny stavu jako zprávy v protokolech serveru mqweb. Každá zpráva označuje ověřený název činitele, který požadoval operaci.

Významné změny stavu, například při vytváření, spouštění, ukončování nebo odstraňování správců front, jsou protokolovány v souborech `messages.log` a `console.log` serveru mqweb na úrovni protokolování [AUDIT]. Každá položka protokolu označuje ověřený název činitele, který požadoval operaci.

Soubory `messages.log` a `console.log` lze nalézt v následujícím umístění:

- V instalaci produktu IBM MQ :
  - Linux AIX V systému AIX nebo Linux: `/var/mqm/web/installations/`*`installationName`*`/servers/mqweb/logs`
  - Windows V systému Windows: *MQ_DATA_PATH*`\web\installations\`*`installationName`*`\servers\mqweb\logs`, kde *MQ_DATA_PATH* je cesta k datům IBM MQ . Tato cesta je cestou k datům, která je vybrána během instalace produktu IBM MQ. Standardně je tato cesta `C:\ProgramData\IBM\MQ`.
- V 9.3.5 Linux V samostatné IBM MQ Web Server instalaci: *MQ_OVERRIDE_DATA_PATH*`/web/installations/MQWEBINST/servers/mqweb/logs`

  kde *MQ_OVERRIDE_DATA_PATH* je datový adresář IBM MQ Web Server , na který odkazuje proměnná prostředí **MQ_OVERRIDE_DATA_PATH** .

Další informace o konfiguraci úrovní protokolování serveru mqweb naleznete v tématu Konfigurace protokolování.

Události příkazu a konfigurace

Volitelně můžete povolit události příkazů a konfigurace ve správci front a poskytnout informace o většině aktivit IBM MQ Console a REST API . Například vytvoření kanálů a dotaz na fronty generují události příkazu a konfigurace. Další informace o povolení událostí příkazu a konfigurace naleznete v tématu Řízení událostí konfigurace, příkazu a modulu protokolování.

Pro tyto zprávy událostí příkazu a konfigurace je pole **MQIACF_EVENT_ORIGIN** nastaveno na hodnotu `MQEVO_REST` a pole **MQCACF_EVENT_APPL_IDENTITY** uvádí prvních 32 znaků ověřeného názvu činitele. Pokud má uživatel roli `MQWebAdmin` nebo `MQWebAdminRO` , pole **MQCACF_EVENT_USER_ID** ohlásí ID uživatele serveru mqweb, nikoli jméno uživatele činitele, který příkaz vydal. Pokud však má uživatel roli `MQWebUser` , **MQCACF_EVENT_USER_ID** ohlásí jméno uživatele činitele, který vydal příkaz.

Související pojmy

“Auditování” na stránce 494
Pomocí zpráv událostí můžete zkontrolovat narušení zabezpečení nebo pokusy o narušení. Můžete také zkontrolovat zabezpečení systému pomocí konzoly IBM MQ Explorer.

Aspekty zabezpečení pro IBM MQ Console a REST API on z/OS

IBM MQ Console a REST API mají funkce zabezpečení, které řídí, zda může uživatel zadávat, zobrazovat nebo měnit příkazy. Příkazy jsou poté předány správci front a zabezpečení správce front je poté použito k řízení, zda má uživatel povoleno zadat příkaz pro daného správce front.

Postup

1. Ujistěte se, že ID uživatele spuštěné úlohy serveru mqweb má příslušná oprávnění k zadání určitých příkazů PCF a přístupu k určitým frontám. Další informace viz téma “Oprávnění požadované ID uživatele spuštěné úlohy serveru mqweb” na stránce 553.

2. Ujistěte se, že všichni uživatelé, kterým byla udělena role `MQWebUser` , mají příslušná oprávnění.

   Uživatelé IBM MQ Console a REST API , kteří jsou přiřazeni k roli `MQWebUser` , pracují v kontextu zabezpečení činitele. Tato ID uživatelů mohou provádět pouze operace, kterým je ID uživatele uděleno pro provádění ve správci front, a je třeba jim udělit přístup ke stejným systémovým frontám jako adresnímu prostoru serveru mqweb.

   ID uživatele spuštěné úlohy serveru mqweb musí mít udělen alternativní přístup ke všem uživatelům přiřazeným k roli `MQWebUser` .

   Další informace o udělení příslušných oprávnění pro uživatele s rolí `MQWebUser` viz "Přístup k prostředkům IBM MQ vyžadovaným pro použití IBM MQ Console nebo REST API" na stránce 553.
3. Volitelné: Nakonfigurujte TLS pro IBM MQ Console a REST API. Další informace viz téma "Konfigurace TLS pro REST API a IBM MQ Console na z/OS" na stránce 555.

z/OS Oprávnění požadované ID uživatele spuštěné úlohy serveru mqweb

V systému z/OSID uživatele spuštěné úlohy serveru mqweb vyžaduje určitá oprávnění k zadání příkazů PCF a přístupu k systémovým prostředkům.

ID uživatele spuštěné úlohy serveru mqweb potřebuje:

- z/OS Identifikátor uživatele systému UNIX (UID), který má být schopen používat z/OS UNIX System Services.
- Přístup k datovým sadám `hlq.SCSQAUTH` a `hlq.SCSQANL*` v instalaci produktu IBM MQ .
- Přístup pro čtení k instalačním souborům produktu IBM MQ v adresáři z/OS UNIX System Services.
- Přístup pro čtení a zápis k uživatelskému adresáři Liberty vytvořenému skriptem **`crtmqweb`** .
- Oprávnění pro připojení ke správci front. Udělte ID uživatele spuštěné úlohy serveru mqweb *READ* přístup k profilu `hlq.BATCH` ve třídě MQCONN.
- Oprávnění k vydávání příkazů IBM MQ a přístupu k určitým frontám. Tyto podrobnosti jsou popsány v části "IBM MQ Console -povinné profily zabezpečení příkazu" na stránce 230, "Zabezpečení systémové fronty" na stránce 206a "Profily pro zabezpečení kontextu" na stránce 217.
- Oprávnění k odběru tématu SYSTEM.FTE , aby bylo možné použít REST API pro MFT. Udělte ID uživatele spuštěné úlohy serveru mqweb *ALTER* přístup k profilu `hlq.SUBSCRIBE.SYSTEM.FTE` ve třídě MXTOPIC.
- Pokud konfigurujete registr SAF, přístup k různým profilům zabezpečení. Další informace viz "Konfigurace registru SAF pro IBM MQ Console a REST API" na stránce 535.

Ověření připojení

Pokud byl váš správce front nakonfigurován tak, aby vyžadoval, aby všechny dávkové aplikace poskytovaly platné ID uživatele a heslo, musíte nastavením parametru CHKLOCL (REQUIRED) udělit ID uživatele spuštěné úlohy *UPDATE* serveru mqweb přístup k profilu `hlq.BATCH` ve třídě MQCONN.

Toto oprávnění způsobí, že ověření připojení bude pracovat v režimu CHKLOCL (OPTIONAL) pro ID uživatele spuštěné úlohy serveru mqweb.

Pokud jste nenakonfigurovali správce front tak, aby vyžadoval, aby všechny dávkové aplikace poskytovaly platné ID uživatele a heslo, stačí udělit ID uživatele, který spouští úlohu serveru mqweb *READ* , přístup k profilu `hlq.BATCH` ve třídě MQCONN.

Další informace o CHCKLOCL viz "Použití produktu CHCKLOCL v lokálně vázaných aplikacích" na stránce 197.

Přístup k prostředkům IBM MQ vyžadovaným pro použití IBM MQ Console nebo REST API

Operace provedené v IBM MQ Consolenebo REST APIuživatelem v roli `MQWebUser` se provádějí v kontextu zabezpečení uživatele.

Informace o této úloze

Další informace o rolích v IBM MQ Console a REST APIviz “Role na IBM MQ Console a REST API” na stránce 537 .

Pomocí následujícího postupu udělte uživateli v roli `MQWebUser` přístup k prostředkům správce front nezbytným pro použití IBM MQ Console nebo REST API.

Postup

1. Udělte ID uživatele `mqweb server started task` alternativní přístup ke každému ID uživatele v roli `MQWebUser` .

   Toto proveďte v každém správci front, kterého budou uživatelé spravovat prostřednictvím konzoly IBM MQ Console nebo konzoly REST API.

   Pomocí následujících ukázkových příkazů RACF můžete uživateli `mqweb server started task` udělit alternativní přístup k uživateli v roli `MQWebUser` :

   ```
   RDEFINE MQADMIN hlq.ALTERNATE.USER.userId UACC(NONE)
   PERMIT hlq.ALTERNATE.USER.userId CLASS(MQADMIN) ACCESS(UPDATE) ID(mqwebUserId)
   SETROPTS RACLIST(MQADMIN) REFRESH
   ```

   kde:

   `hlq`
   Předpona profilu, která může být buď názvem správce front, nebo názvem skupiny sdílení front.

   `userId`
   Je uživatel v roli `MQWebUser`

   `mqwebUserId`
   Je ID uživatele `mqweb server started task`

   Poznámka: Používáte-li zabezpečení s různými případy, použijte třídu MXADMIN spíše než třídu MQADMIN.
2. Udělte každému uživateli v roli `MQWebUser` přístup k systémovým frontám, které jsou nezbytné pro použití IBM MQ Console a REST API.

   Chcete-li to provést, pro systém SYSTEM.ADMIN.COMMAND.QUEUE a SYSTEM.REST.REPLY.QUEUE, udělte každému uživateli přístup UPDATE ke třídám MQQUEUE nebo MXQUEUE, v závislosti na tom, zda se používá zabezpečení s různými případy.

   To je třeba provést pro každého správce front, kterého bude uživatel spravovat prostřednictvím konzoly REST API, včetně vzdálených správců front spravovaných prostřednictvím konzoly Komunikační brána administrative REST API.
3. Chcete-li uživateli v roli `MQWebUser` povolit administraci vzdálených správců front, udělte uživateli přístup UPDATE k profilu ve třídě MQQUEUE nebo MXQUEUE, čímž chráníte přenosovou frontu používanou k odesílání příkazů vzdálenému správci front. Všimněte si, že musíte uživateli udělit přístup UPDATE ke správci front brány.

   Ve vzdáleném správci front udělte přístup stejnému uživateli pro vložení do přenosové fronty použité k odeslání zpráv odezvy příkazu zpět správci front brány.
4. Udělte uživatelům v roli `MQWebUser` přístup k jakýmkoli dalším prostředkům, které jsou nezbytné k provedení operací podporovaných IBM MQ Console a REST API.

   Přístup potřebný k:

   - Operace provedení v produktu REST APIjsou popsány v sekcích *Požadavky zabezpečení* jednotlivých REST API prostředků .
   - Zadání příkazů pomocí příkazu IBM MQ Console je popsáno v tématu “IBM MQ Console -povinné profily zabezpečení příkazu” na stránce 230 .

z/OS Konfigurace TLS pro REST API a IBM MQ Console na z/OS

V systému z/OSmůžete nakonfigurovat server mqweb tak, aby používal svazek klíčů RACF k ukládání certifikátů pro zabezpečená připojení pomocí protokolu TLS a ověřování klientských certifikátů.

Než začnete

Chcete-li provést tento postup, musíte být uživatelem, který má přístup pro zápis k souboru `mqwebuser.xml` a oprávnění pro práci se svazky klíčů SAF.

Informace o této úloze

Výchozí konfigurace serveru mqweb používá úložiště klíčů Java pro server a důvěryhodné certifikáty. V systému z/OSmůžete nakonfigurovat server mqweb tak, aby místo úložiště klíčů Java používal svazek klíčů RACF . Server lze také nakonfigurovat tak, aby umožňoval uživatelům ověřování pomocí certifikátu klienta.

Informace o použití RACF kroužků klíčů v Libertyviz Liberty: Keystores .

Postupujte takto, chcete-li nakonfigurovat server mqweb tak, aby používal svazek klíčů RACF , a volitelně nakonfigurujte ověření pomocí certifikátu klienta. Tento postup popisuje kroky nezbytné pro vytvoření a použití certifikátů podepsaných s vlastními certifikáty certifikační autority (CA). V produkčním prostředí můžete raději používat certifikáty získané od externí certifikační autority.

Postup

1. Vytvořte certifikát certifikační autority (CA), který bude použit k podepsání certifikátu serveru. Zadejte například následující příkaz RACF :

   ```
   RACDCERT GENCERT -
     CERTAUTH -
     SUBJECTSDN(CN('mqweb Certification Authority') -
       O('IBM') -
       OU('MQ')) -
     SIZE(2048) -
     WITHLABEL('mqwebCertauth')
   ```

2. Vytvořte certifikát serveru podepsaný certifikátem CA vytvořeným v kroku 1 zadáním následujícího příkazu:

   ```
   RACDCERT ID(mqwebUserId) GENCERT -
     SUBJECTSDN(CN('hostname') -
      O('IBM') -
      OU('MQ')) -
      SIZE(2048) -
      SIGNWITH (CERTAUTH LABEL('mqwebCertauth')) -
     WITHLABEL('mqwebServerCert')
   ```

   kde *mqwebUserId* je ID uživatele spuštěné úlohy serveru mqweb a *hostname* je název hostitele serveru mqweb.

3. Připojte certifikát CA a certifikát serveru ke svazku klíčů SAF zadáním následujících příkazů:

   ```
   RACDCERT ID(mqwebUserId) CONNECT(RING(keyring) LABEL('mqwebCertauth') CERTAUTH)
   RACDCERT ID(mqwebUserId) CONNECT(RING(keyring) LABEL('mqwebServerCert'))
   ```

   kde *mqwebUserId* je ID uživatele spuštěné úlohy serveru mqweb a *keyring* je název svazku klíčů, který chcete použít.

4. Exportujte certifikát CA do souboru CER zadáním následujícího příkazu:

   ```
   RACDCERT CERTAUTH EXPORT(LABEL('mqwebCertauth')) -
           DSN('hlq.CERT.MQWEBCA') -
           FORMAT(CERTDER) -
           PASSWORD('password')
   ```

5. Přeneste exportovaný certifikát certifikační autority prostřednictvím protokolu FTP v binárním formátu na pracovní stanici a importujte jej do prohlížeče jako certifikát certifikační autority.

6. Volitelné: Chcete-li konfigurovat ověření klientského certifikátu, vytvořte a exportujte klientský certifikát.
   a) Vytvořte certifikát certifikační autority (CA), který se použije k podepsání certifikátu klienta. Zadejte například následující příkaz RACF :

```
RACDCERT GENCERT -
  CERTAUTH -
  SUBJECTSDN(CN('mqweb User CA') -
   O('IBM') -
   OU('MQ')) -
   SIZE(2048) -
  WITHLABEL('mqwebUserCertauth')
```

   b) Připojte certifikát CA ke svazku klíčů SAF zadáním následujícího příkazu:

```
RACDCERT ID(mqwebUserId) CONNECT(RING(keyring) LABEL('mqwebUserCertauth') CERTAUTH)
```

   kde *mqwebUserId* je ID uživatele spuštěné úlohy serveru mqweb a *keyring* je název svazku klíčů, který chcete použít.

   c) Vytvořte certifikát klienta podepsaný certifikátem CA. Můžete například použít následující příkaz:

```
RACDCERT ID(clientUserId) GENCERT -
  SUBJECTSDN(CN('clientUserId') -
     O('IBM') -
     OU('MQ')) -
   SIZE(2048) -
   SIGNWITH (CERTAUTH LABEL('mqwebUserCertauth')) -
  WITHLABEL('userCertLabel')
```

   kde *clientUserId* je jméno uživatele.

   Metoda použitá k mapování certifikátu na činitele závisí na typu konfigurovaného registru uživatelů:

   - Pokud používáte základní registr, pole Obecný název v certifikátu se shoduje s uživatelem v registru.
   - Používáte-li registr SAF a certifikát se nachází v databázi RACF , použije se vlastník certifikátu určený parametrem **ID** při vytváření certifikátu.
   - Pokud používáte registr LDAP, je úplný rozlišující název v certifikátu porovnán s registrem LDAP.

   d) Exportujte certifikát klienta do souboru PKCS #12 zadáním následujícího příkazu:

```
RACDCERT ID(mqwebUserId) EXPORT(LABEL('userCertLabel')) -
         PASSWORD('password') DSN('hlq.USER.CERT')
```

   e) Přeneste exportovaný certifikát v binárním formátu na vaši pracovní stanici pomocí protokolu FTP. Chcete-li použít certifikát klienta s produktem IBM MQ Console, naimportujte jej do webového prohlížeče použitého pro přístup k produktu IBM MQ Console jako osobní certifikát.
7. Upravte soubor *WLP_user_directory*/servers/mqweb/mqwebuser.xml, kde *WLP_user_directory* je adresář, který byl určen při spuštění skriptu **crtmqweb** pro vytvoření definice serveru mqweb.

   Proveďte následující změny a nakonfigurujte server mqweb tak, aby používal svazek klíčů RACF :

   a) Odeberte nebo označte jako komentář následující řádek:

```
<sslDefault sslRef="mqDefaultSSLConfig"/>
```

   b) Přidejte následující příkazy:

```
<keyStore id="defaultKeyStore" filebased="false"
          location="safkeyring://mqwebUserId/keyring"
          password="password" readOnly="true" type="JCERACFKS" />
<ssl id="thisSSLConfig" keyStoreRef="defaultKeyStore" sslProtocol="TLSv1.2"
          serverKeyAlias="mqwebServerCert" clientAuthenticationSupported="true" />
<sslDefault sslRef="thisSSLConfig"/>
```

   kde:

   - *mqwebUserId* je ID uživatele spuštěné úlohy serveru mqweb.

- *svazek klíčů* je název svazku klíčů RACF .
- *mqwebServerCert* je popisek certifikátu serveru mqweb.

Notes: Hodnota **keyStore password** je ignorována.

8. Restartujte server mqweb zastavením a restartováním spuštěné úlohy serveru mqweb.
9. Volitelné: Použít certifikát klienta k ověření:
   - Chcete-li použít certifikát klienta s produktem IBM MQ Console, zadejte URL pro IBM MQ Console ve webovém prohlížeči, kde jste nainstalovali certifikát klienta.
   - Chcete-li použít certifikát klienta s rozhraním REST API, poskytněte certifikát klienta s každým požadavkem REST.

   Notes:

   a. Pokud k ověření v produktu IBM MQ Consolepoužíváte pouze certifikáty, může prohlížeč zobrazit seznam certifikátů, ze kterých si můžete vybrat.

   b. Chcete-li použít jiný certifikát, možná budete muset zavřít a restartovat prohlížeč.

   c. Pokud používáte certifikáty klienta, které nejsou v databázi RACF , můžete použít filtrování názvů certifikátů RACF k mapování atributů certifikátů na ID uživatele. Příklad:

   ```
   RACDCERT ID(DEPT3USR) MAP SDNFILTER(OU=DEPT1.C=US)
   ```

   mapuje certifikáty s rozlišujícím názvem subjektu, který obsahuje OU=DEPT1 a C=US , na ID uživatele DEPT3USR.

Výsledky

Nastavili jste rozhraní TLS pro IBM MQ Console a REST API.

ALW Správa klíčů a certifikátů v systému AIX, Linux, and Windows

V systému AIX, Linux, and Windowspoužijte příkazy **runmqckm** a **runmqakm** ke správě klíčů, certifikátů a požadavků na certifikáty.

Informace o této úloze

Příkaz **runmqckm** poskytuje funkce, které jsou podobné funkcím **iKeyman**, a příkaz **runmqakm** poskytuje funkce, které jsou podobné funkcím **gskitcapicmd**. Před použitím **runmqckm** nebo **runmqakm**se ujistěte, že systémové proměnné prostředí jsou správně nakonfigurovány spuštěním příkazu **setmqenv** .

Příkaz **runmqckm** vyžaduje instalaci komponenty IBM MQ JRE. Není-li tato komponenta nainstalována, můžete použít příkaz **runmqakm** .

Potřebujete-li spravovat certifikáty TLS způsobem, který vyhovuje standardu FIPS, použijte příkaz **runmqakm** namísto příkazu **runmqckm** . Důvodem je, že příkaz **runmqakm** podporuje silnější šifrování.

Procedura

- Pomocí příkazů **runmqckm** a **runmqakm** proveďte následující akce:
  - V 9.3.0 Vytvořte typ souborů databáze klíčů CMS nebo PKCS#12 , které produkt IBM MQ vyžaduje
  - Vytvořit žádosti o certifikát
  - Importovat osobní certifikáty
  - Importovat certifikáty CA
  - Spravovat certifikáty podepsané sebou samým

Související úlohy

"Použití uživatelského rozhraní produktu strmqikm" na stránce 308

Osobní certifikát můžete vytvořit pomocí **strmqikm** (iKeyman) Grafické uživatelské rozhraní.

Související odkazy

Vyvolání grafického uživatelského rozhraní IBM **strmqikm** (iKeyman)

Související informace

Nástroj Keytool

ALW příkazy runmqckm a runmqakm na systému AIX, Linux, and Windows

Tento oddíl popisuje příkazy **runmqckm** a **runmqakm** podle objektu příkazu.

Hlavní rozdíly mezi těmito dvěma příkazy jsou následující:

- **runmqckm**
  - Poskytuje funkce, které jsou podobné funkcím **iKeycmd** .
  - Podporuje formáty souborů úložiště klíčů JKS a JCEKS.
- **runmqakm**
  - Poskytuje funkce, které jsou podobné funkcím **gskitcapicmd** .
  - Podporuje vytváření certifikátů a žádostí o certifikáty pomocí veřejných klíčů Elliptic Curve, zatímco příkaz **runmqckm** nikoli.
  - Podporuje silnější šifrování souboru úložiště klíčů než příkaz **runmqckm** prostřednictvím parametru **-strong** .
  - Byl certifikován jako vyhovující FIPS 140-2 a lze jej nakonfigurovat tak, aby fungoval v souladu se standardem FIPS, pomocí parametru **-fips** .

Upozornění: Příkaz **runmqckm** vyžaduje instalaci funkce IBM MQ Java runtime environment (JRE).

Každý příkaz uvádí alespoň jeden *objekt*. Příkazy pro operace zařízení PKCS #11 mohou určovat další objekty. Příkazy pro objekty databáze klíčů, certifikátu a žádosti o certifikát také uvádějí *akci*. Objekt může být jeden z následujících:

-keydb
Akce se vztahují na databázi klíčů

-cert
Akce se vztahují na certifikát

-certreq-počet
Akce se vztahují na žádost o certifikát

-help
Zobrazí nápovědu.

-version
Zobrazí informace o verzi

Následující dílčí témata popisují akce, které můžete provést s objekty databáze klíčů, certifikátu a žádosti o certifikát. Popis voleb pro tyto příkazy naleznete v části "Volby runmqckm a runmqakm na systému AIX, Linux, and Windows" na stránce 570 .

ALW Příkazy pro databáze klíčů CMS nebo PKCS#12 na systému AIX, Linux, and Windows

Pomocí příkazů **runmqckm** a **runmqakm** můžete spravovat klíče a certifikáty pro databázi klíčů CMS nebo databázi klíčů PKCS#12 .

Poznámka: Produkt IBM MQ nepodporuje algoritmy SHA-3 nebo SHA-5 . Můžete použít názvy algoritmů digitálního podpisu SHA384WithRSA a SHA512WithRSA , protože oba algoritmy jsou členy řady SHA-2 .

Deprecated Názvy algoritmů digitálního podpisu SHA3WithRSA a SHA5WithRSA jsou zamítnuty, protože se jedná o zkrácenou formu SHA384WithRSA a SHA512WithRSA .

-keydb -changepw
Změňte heslo pro databázi klíčů:

Pomocí příkazu **runmqckm** :

```
-keydb -changepw -db filename -pw password -new_pw new_password -expire days
```

Pomocí příkazu **runmqakm** :

```
-keydb -changepw -db filename -pw password -new_pw new_password -expire days
-fips -strong
```

-keydb -převést
Pro příkaz **runmqckm** převeďte databázi klíčů z jednoho formátu do jiného:

```
-keydb -convert -db filename -pw password
-old_format cms | pkcs12 -new_format cms
```

Pomocí příkazu **runmqakm** převeďte starou verzi databáze klíčů CMS na novou verzi databáze klíčů CMS :

```
-keydb -convert -db filename -pw password
-new_db filename -new_pw password -strong -fips
```

-keydb -vytvořit
Vytvořte databázi klíčů:

Pomocí příkazu **runmqckm** :

V 9.3.0 `-keydb -create -db filename -pw password -type cms
| pkcs12`

Pomocí příkazu **runmqakm** :

V 9.3.0 `-keydb -create -db filename -pw password -type cms
/ p12 -fips -strong`

-keydb -odstranění
Odstranit databázi klíčů:

Pomocí jednoho z těchto příkazů:

```
-keydb -delete -db filename -pw password
```

-keydb -seznam
Seznam aktuálně podporovaných typů databáze klíčů:

Pomocí příkazu **runmqckm** :

```
-keydb -list
```

Pomocí příkazu **runmqakm** :

```
-keydb -list -fips
```

-cert -přidat
Přidejte certifikát ze souboru do databáze klíčů:

Pomocí příkazu **runmqckm** :

```
-cert -add -db filename -pw password -label label -file filename
-format ascii | binary
```

Pomocí příkazu **runmqakm** :

```
-cert -add -db filename -pw password -label label -file filename
-format ascii | binary -fips
```

-cert -vytvořit

Vytvořte certifikát podepsaný svým držitelem:

Pomocí příkazu **runmqckm** :

```
-cert -create -db filename -pw password -label label
-dn distinguished_name -size 1024 | 512 -x509version 3 | 1 | 2
-expire days -sig_alg MD2_WITH_RSA | MD2WithRSA |
MD5_WITH_RSA | MD5WithRSA |
SHA1WithDSA | SHA1WithRSA |
SHA256_WITH_RSA | SHA256WithRSA |
SHA2WithRSA | SHA384_WITH_RSA |
SHA384WithRSA | SHA512_WITH_RSA |
SHA512WithRSA | SHA_WITH_DSA |
SHA_WITH_RSA | SHAWithDSA |
SHAWithRSA
```

Pomocí příkazu **runmqakm** :

```
-cert -create -db filename -pw password -label label
-dn distinguished_name -size 2048 | 1024 | 512 -x509version 3 | 1 | 2
-expire days -fips -sig_alg md5 |
MD5_WITH_RSA | SHA_WITH_DSA |
SHA_WITH_RSA | sha1 |
SHA1WithDSA | SHA1WithECDSA |
SHA1WithRSA | sha224 |
SHA224_WITH_RSA | SHA224WithDSA |
SHA224WithECDSA | SHA224WithRSA |
sha256 | SHA256_WITH_RSA |
SHA256WithDSA | SHA256WithECDSA |
SHA256WithRSA | SHA2WithRSA |
sha384 | SHA384_WITH_RSA |
SHA384WithECDSA | SHA384WithRSA |
sha512 | SHA512_WITH_RSA |
SHA512WithECDSA | SHA512WithRSA |
SHAWithDSA | SHAWithRSA |
EC_ecdsa_with_SHA1 | EC_ecdsa_with_SHA224 |
EC_ecdsa_with_SHA256 | EC_ecdsa_with_SHA384 |
EC_ecdsa_with_SHA512
```

-cert -odstranění

Odstranit certifikát:

Pomocí příkazu **runmqckm** :

```
-cert -delete -db filename -pw password -label label
```

Pomocí příkazu **runmqakm** :

```
-cert -delete -db filename -pw password -label label -fips
```

-cert -podrobné informace

Vypište podrobné informace o konkrétním certifikátu:

Pomocí příkazu **runmqckm** :

```
-cert -details -db filename -pw password -label label
```

Pomocí příkazu **runmqakm** :

```
-cert -details -db filename -pw password -label label -fips
```

-cert -exportovat
Exportujte osobní certifikát a jeho přidružený soukromý klíč z databáze klíčů do souboru PKCS#12 nebo do jiné databáze klíčů:

Pomocí příkazu **runmqckm** :

```
-cert -export -db filename -pw password -label label -type cms | pkcs12
-target filename -target_pw password -target_type  cms | pkcs12
```

Pomocí příkazu **runmqakm** :

```
-cert -export -db filename -pw password -label label -type cms | pkcs12
-target filename -target_pw password -target_type  cms | pkcs12
-encryption strong | weak -fips
```

-cert -extrakt
Extrahujte certifikát z databáze klíčů:

Pomocí příkazu **runmqckm** :

```
-cert -extract -db filename -pw password -label label -target filename
-format ascii | binary
```

Pomocí příkazu **runmqakm** :

```
-cert -extract -db filename -pw password -label label -target filename
-format ascii | binary -fips
```

-cert -import
Import osobního certifikátu z databáze klíčů:

Pomocí příkazu **runmqckm** :

```
-cert -import -file filename -pw password -type pkcs12 -target filename
-target_pw password -target_type cms -label  label
```

Pomocí příkazu **runmqakm** :

```
-cert -import -file filename -pw password -type cms -target filename
-target_pw password -target_type cms -label  label -fips
```

Pro oba tyto příkazy:

- Volba `-label` je povinná a uvádí popisek certifikátu, který se má importovat ze zdrojové databáze klíčů.
- Dále můžete použít volbu `-new_label` . To umožňuje, aby byl importovanému certifikátu ve zdrojové databázi udělen jiný popisek v cílové databázi klíčů než popisek ve zdrojové databázi.

-cert -seznam
Seznam všech certifikátů v databázi klíčů:

Pomocí příkazu **runmqckm** :

```
-cert -list all | personal | CA -db filename -pw password
```

Pomocí příkazu **runmqakm** :

```
-cert -list all | personal | CA -db filename -pw password -fips
```

-cert -příjem
Přijmout certifikát ze souboru:

Pomocí příkazu **runmqckm** :

```
-cert -receive -file filename -db filename -pw password
-format ascii | binary -default_cert yes | no
```

Pomocí příkazu **runmqakm** :

```
-cert -receive -file filename -db filename -pw password
-format ascii | binary -default_cert yes | no -fips
```

-cert -znamení

Podepsat certifikát:

Pomocí příkazu **runmqckm** :

```
-cert -sign -db filename -file filename -pw password
-label label -target filename -format ascii | binary -expire days
-sig_alg MD2_WITH_RSA | MD2WithRSA | MD5_WITH_RSA |
MD5WithRSA | SHA1WithDSA | SHA1WithRSA |
SHA256_WITH_RSA | SHA256WithRSA |
SHA2WithRSA | SHA384_WITH_RSA |
SHA384WithRSA | SHA512_WITH_RSA |
SHA512WithRSA | SHA_WITH_DSA |
SHA_WITH_RSA | SHAWithDSA |
SHAWithRSA
```

Pomocí příkazu **runmqakm** :

```
-cert -sign -db filename -file filename -pw password
-label label -target filename -format ascii | binary -expire days -fips
-sig_alg md5 | MD5_WITH_RSA | SHA_WITH_DSA |
SHA_WITH_RSA | sha1 | SHA1WithDSA |
SHA1WithECDSA | SHA1WithRSA | sha224 |
SHA224_WITH_RSA | SHA224WithDSA |
SHA224WithECDSA | SHA224WithRSA | sha256 |
SHA256_WITH_RSA | SHA256WithDSA |
SHA256WithECDSA | SHA256WithRSA |
SHA2WithRSA | sha384 | SHA384_WITH_RSA |
SHA384WithECDSA | SHA384WithRSA |
sha512 | SHA512_WITH_RSA |
SHA512WithECDSA | SHA512WithRSA |
SHAWithDSA | SHAWithRSA |
EC_ecdsa_with_SHA1 | EC_ecdsa_with_SHA224 |
EC_ecdsa_with_SHA256 | EC_ecdsa_with_SHA384 |
EC_ecdsa_with_SHA512
```

-certreq -vytvořit

Vytvořte žádost o certifikát:

Pomocí příkazu **runmqckm** :

```
-certreq -create -db filename -pw password -label label -dn distinguished_name
-size 1024 | 512 -file filename
-sig_alg MD2_WITH_RSA | MD2WithRSA |
MD5_WITH_RSA | MD5WithRSA |
SHA1WithDSA | SHA1WithRSA |
SHA256_WITH_RSA | SHA256WithRSA |
SHA2WithRSA | SHA384_WITH_RSA |
SHA384WithRSA | SHA512_WITH_RSA |
SHA512WithRSA | SHA_WITH_DSA |
SHA_WITH_RSA | SHAWithDSA |
SHAWithRSA
```

Pomocí příkazu **runmqakm** :

```
-certreq -create -db filename -pw password -label label -dn distinguished_name
-size 2048 | 1024 | 512 -file filename -fips
-sig_alg md5 | MD5_WITH_RSA | SHA_WITH_DSA |
SHA_WITH_RSA | sha1 | SHA1WithDSA |
SHA1WithECDSA | SHA1WithRSA | sha224 |
SHA224_WITH_RSA | SHA224WithDSA |
SHA224WithECDSA | SHA224WithRSA | sha256 |
SHA256_WITH_RSA | SHA256WithDSA |
SHA256WithECDSA | SHA256WithRSA |
```

```
SHA2WithRSA | sha384 | SHA384_WITH_RSA |
SHA384WithECDSA | SHA384WithRSA |
sha512 | SHA512_WITH_RSA |
SHA512WithECDSA | SHA512WithRSA |
SHAWithDSA | SHAWithRSA |
EC_ecdsa_with_SHA1 | EC_ecdsa_with_SHA224 |
EC_ecdsa_with_SHA256 | EC_ecdsa_with_SHA384 |
EC_ecdsa_with_SHA512
```

-certreq -odstranění
Odstranit žádost o certifikát:

Pomocí příkazu **runmqckm** :

```
-certreq -delete -db filename -pw password -label  label
```

Pomocí příkazu **runmqakm** :

```
-certreq -delete -db filename -pw password -label  label -fips
```

-certreq -podrobnosti
Seznam podrobných informací o konkrétní žádosti o certifikát:

Pomocí příkazu **runmqckm** :

```
-certreq -details -db filename -pw password -label  label
```

Pomocí příkazu **runmqakm** :

```
-certreq -details -db filename -pw password -label  label -fips
```

Vypište podrobné informace o žádosti o certifikát a zobrazte úplnou žádost o certifikát:

Pomocí příkazu **runmqckm** :

```
-certreq -details -showOID -db filename -pw password -label label
```

Pomocí příkazu **runmqakm** :

```
-certreq -details -showOID -db filename -pw password -label label -fips
```

-certreq -extrakt
Extrahujte žádost o certifikát z databáze žádostí o certifikát do souboru:

Pro příkaz **runmqckm** :

```
-certreq -extract -db filename -pw password -label label -target filename
```

Pomocí příkazu **runmqakm** :

```
-certreq -extract -db filename -pw password -label label -target filename -fips
```

-certreq -seznam
Seznam všech žádostí o certifikát v databázi žádostí o certifikát:

Pomocí příkazu **runmqckm** :

```
-certreq -list -db filename -pw password
```

Pomocí příkazu **runmqakm** :

```
-certreq -list -db filename -pw password -fips
```

-certreq -znovu vytvořit
Znovu vytvořte žádost o certifikát:

Pomocí příkazu **runmqckm** :

```
-certreq -recreate -db filename -pw password -label label -target filename
```

Pomocí příkazu **runmqakm** :

```
-certreq -recreate -db filename -pw password -label label -target filename -fips
```

ALW Příkazy pro operace šifrovacího zařízení na systému AIX, Linux, and Windows

Ke správě klíčů a certifikátů pro operace šifrovacího zařízení můžete použít příkazy **runmqckm** (iKeycmd) a **runmqakm** .

Poznámka: Produkt IBM MQ nepodporuje algoritmy SHA-3 nebo SHA-5 . Můžete použít názvy algoritmů digitálního podpisu SHA384WithRSA a SHA512WithRSA , protože oba algoritmy jsou členy řady SHA-2 .

Deprecated Názvy algoritmů digitálního podpisu SHA3WithRSA a SHA5WithRSA jsou zamítnuty, protože se jedná o zkrácenou formu SHA384WithRSA a SHA512WithRSA .

-keydb -changepw
Změňte heslo pro šifrovací zařízení:

Pomocí příkazu **runmqckm** :

```
-keydb -changepw -crypto module_name -tokenlabel token_label
-pw password -new_pw new_password
```

Používáte-li certifikáty nebo klíče uložené na šifrovacím hardwaru PKCS#11 , mějte na paměti, že **runmqckm** a **strmqikm** jsou 64bitové programy. Externí moduly požadované pro podporu PKCS#11 budou načteny do 64bitového procesu, proto musíte mít nainstalovanou 64bitovou knihovnu PKCS#11 pro administraci šifrovacího hardwaru. 32bitové platformy Windows a Linux x86 jsou jedinými výjimkami, protože programy **strmqikm** a **runmqckm** jsou na těchto platformách 32bitové.

Pomocí příkazu **runmqakm** :

```
-keydb -changepw -db filename -crypto module_name -tokenlabel  token_label
-pw password -new_pw new_password -fips -strong
```

-keydb -seznam
Seznam aktuálně podporovaných typů databáze klíčů:

Pomocí příkazu **runmqckm** :

```
-keydb -list
```

Používáte-li certifikáty nebo klíče uložené na šifrovacím hardwaru PKCS#11 , mějte na paměti, že **runmqckm** a **strmqikm** jsou 64bitové programy. Externí moduly požadované pro podporu PKCS#11 budou načteny do 64bitového procesu, proto musíte mít nainstalovanou 64bitovou knihovnu PKCS#11 pro administraci šifrovacího hardwaru. 32bitové platformy Windows a Linux x86 jsou jedinými výjimkami, protože programy **strmqikm** a **runmqckm** jsou na těchto platformách 32bitové.

Pomocí příkazu **runmqakm** :

```
-keydb -list -fips
```

-cert -přidat
Přidejte certifikát ze souboru do šifrovacího zařízení:

Pomocí příkazu **runmqckm** :

```
-cert -add -crypto module_name -tokenlabel token_label -pw password
-label label -file filename -format ascii | binary
```

Používáte-li certifikáty nebo klíče uložené na šifrovacím hardwaru PKCS#11 , mějte na paměti, že **runmqckm** a **strmqikm** jsou 64bitové programy. Externí moduly požadované pro podporu PKCS#11 budou načteny do 64bitového procesu, proto musíte mít nainstalovanou 64bitovou knihovnu PKCS#11 pro administraci šifrovacího hardwaru. 32bitové platformy Windows a Linux x86 jsou jedinými výjimkami, protože programy **strmqikm** a **runmqckm** jsou na těchto platformách 32bitové.

Pomocí příkazu **runmqakm** :

```
-cert -add -crypto module_name -tokenlabel token_label -pw password
-label label -file filename -format ascii | binary -fips
```

-cert -vytvořit

Vytvořte certifikát podepsaný svým držitelem na šifrovacím zařízení:

Pomocí příkazu **runmqckm** :

```
-cert -create -crypto module_name -tokenlabel token_label
-pw password -label label -dn distinguished_name
-size 1024 | 512 -x509version 3 | 1 | 2
-default_cert no | yes -expire days
-sig_alg MD2_WITH_RSA | MD2WithRSA |
MD5_WITH_RSA | MD5WithRSA |
SHA1WithDSA | SHA1WithRSA |
SHA256_WITH_RSA | SHA256WithRSA |
SHA2WithRSA | SHA384_WITH_RSA |
SHA384WithRSA | SHA512_WITH_RSA |
SHA512WithRSA | SHA_WITH_DSA |
SHA_WITH_RSA | SHAWithDSA |
SHAWithRSA
```

Používáte-li certifikáty nebo klíče uložené na šifrovacím hardwaru PKCS#11 , mějte na paměti, že **runmqckm** a **strmqikm** jsou 64bitové programy. Externí moduly požadované pro podporu PKCS#11 budou načteny do 64bitového procesu, proto musíte mít nainstalovanou 64bitovou knihovnu PKCS#11 pro administraci šifrovacího hardwaru. 32bitové platformy Windows a Linux x86 jsou jedinými výjimkami, protože programy **strmqikm** a **runmqckm** jsou na těchto platformách 32bitové.

Pomocí příkazu **runmqakm** :

```
-cert -create -crypto module_name -tokenlabel token_label
-pw password -label label -dn distinguished_name
-size 2048 | 1024 | 512 -x509version 3 | 1 | 2
-default_cert no | yes -expire days
-fips -sig_alg md5 | MD5_WITH_RSA | SHA_WITH_DSA |
SHA_WITH_RSA | sha1 | SHA1WithDSA |
SHA1WithECDSA | SHA1WithRSA |
sha224 | SHA224_WITH_RSA |
SHA224WithDSA | SHA224WithECDSA |
SHA224WithRSA | sha256 |
SHA256_WITH_RSA | SHA256WithDSA |
SHA256WithECDSA | SHA256WithRSA |
SHA2WithRSA | sha384 | SHA384_WITH_RSA |
SHA384WithECDSA | SHA384WithRSA |
sha512 | SHA512_WITH_RSA |
SHA512WithECDSA | SHA512WithRSA |
SHAWithDSA | SHAWithRSA |
EC_ecdsa_with_SHA1 | EC_ecdsa_with_SHA224 |
EC_ecdsa_with_SHA256 | EC_ecdsa_with_SHA384 |
EC_ecdsa_with_SHA512
```

-cert -odstranění

Odstranění certifikátu na šifrovacím zařízení:

Pomocí příkazu **runmqckm** :

```
-cert -delete -crypto module_name -tokenlabel token_label -pw password -label label
```

Používáte-li certifikáty nebo klíče uložené na šifrovacím hardwaru PKCS#11 , mějte na paměti, že **runmqckm** a **strmqikm** jsou 64bitové programy. Externí moduly požadované pro podporu PKCS#11 budou načteny do 64bitového procesu, proto musíte mít nainstalovanou 64bitovou knihovnu

PKCS#11 pro administraci šifrovacího hardwaru. 32bitové platformy Windows a Linux x86 jsou jedinými výjimkami, protože programy **strmqikm** a **runmqckm** jsou na těchto platformách 32bitové.

Pomocí příkazu **runmqakm** :

```
-cert -delete -crypto module_name -tokenlabel token_label -pw password -label label -fips
```

-cert -podrobné informace
Vypsat podrobné informace pro specifický certifikát na šifrovacím zařízení:

Pomocí příkazu **runmqckm** :

```
-cert -details -crypto module_name -tokenlabel token_label
-pw password -label label
```

Používáte-li certifikáty nebo klíče uložené na šifrovacím hardwaru PKCS#11 , mějte na paměti, že **runmqckm** a **strmqikm** jsou 64bitové programy. Externí moduly požadované pro podporu PKCS#11 budou načteny do 64bitového procesu, proto musíte mít nainstalovanou 64bitovou knihovnu PKCS#11 pro administraci šifrovacího hardwaru. 32bitové platformy Windows a Linux x86 jsou jedinými výjimkami, protože programy **strmqikm** a **runmqckm** jsou na těchto platformách 32bitové.

Pomocí příkazu **runmqakm** :

```
-cert -details -crypto module_name -tokenlabel token_label
-pw password -label label -fips
```

Vypište podrobné informace a zobrazte úplný certifikát pro specifický certifikát na šifrovacím zařízení:

Pomocí příkazu **runmqckm** :

```
-cert -details -showOID -crypto module_name -tokenlabel  token_label
-pw password -label label
```

Používáte-li certifikáty nebo klíče uložené na šifrovacím hardwaru PKCS#11 , mějte na paměti, že **runmqckm** a **strmqikm** jsou 64bitové programy. Externí moduly požadované pro podporu PKCS#11 budou načteny do 64bitového procesu, proto musíte mít nainstalovanou 64bitovou knihovnu PKCS#11 pro administraci šifrovacího hardwaru. 32bitové platformy Windows a Linux x86 jsou jedinými výjimkami, protože programy **strmqikm** a **runmqckm** jsou na těchto platformách 32bitové.

Pomocí příkazu **runmqakm** :

```
-cert -details -showOID -crypto module_name -tokenlabel  token_label
-pw password -label label -fips
```

-cert -extrakt
Extrahujte certifikát z databáze klíčů:

Pomocí příkazu **runmqckm** :

```
-cert -extract -crypto module_name -tokenlabel token_label -pw password
-label label -target filename -format ascii | binary
```

Používáte-li certifikáty nebo klíče uložené na šifrovacím hardwaru PKCS#11 , mějte na paměti, že **runmqckm** a **strmqikm** jsou 64bitové programy. Externí moduly požadované pro podporu PKCS#11 budou načteny do 64bitového procesu, proto musíte mít nainstalovanou 64bitovou knihovnu PKCS#11 pro administraci šifrovacího hardwaru. 32bitové platformy Windows a Linux x86 jsou jedinými výjimkami, protože programy **strmqikm** a **runmqckm** jsou na těchto platformách 32bitové.

Pomocí příkazu **runmqakm** :

```
-cert -extract -crypto module_name -tokenlabel token_label -pw password
-label label -target filename -format ascii | binary -fips
```

-cert -import
Importovat certifikát do šifrovacího zařízení s podporou sekundární databáze klíčů:

Pomocí příkazu **runmqckm** :

```
-cert -import -db filename -pw password -label label -type cms
-crypto module_name -tokenlabel token_label -pw  password
-secondaryDB filename -secondaryDBpw password
```

Používáte-li certifikáty nebo klíče uložené na šifrovacím hardwaru PKCS#11 , mějte na paměti, že **runmqckm** a **strmqikm** jsou 64bitové programy. Externí moduly požadované pro podporu PKCS#11 budou načteny do 64bitového procesu, proto musíte mít nainstalovanou 64bitovou knihovnu PKCS#11 pro administraci šifrovacího hardwaru. 32bitové platformy Windows a Linux x86 jsou jedinými výjimkami, protože programy **strmqikm** a **runmqckm** jsou na těchto platformách 32bitové.

Pomocí příkazu **runmqakm** :

```
-cert -import -db filename -pw password -label label -type cms
-crypto module_name -tokenlabel token_label -pw  password
-secondaryDB filename -secondaryDBpw password -fips
```

Import certifikátu PKCS #12 do šifrovacího zařízení s podporou sekundární databáze klíčů:

Pomocí příkazu **runmqckm** :

```
-cert -import -file filename -pw password -type pkcs12
-crypto module_name -tokenlabel token_label -pw  password
-secondaryDB filename -secondaryDBpw password
```

Používáte-li certifikáty nebo klíče uložené na šifrovacím hardwaru PKCS#11 , mějte na paměti, že **runmqckm** a **strmqikm** jsou 64bitové programy. Externí moduly požadované pro podporu PKCS#11 budou načteny do 64bitového procesu, proto musíte mít nainstalovanou 64bitovou knihovnu PKCS#11 pro administraci šifrovacího hardwaru. 32bitové platformy Windows a Linux x86 jsou jedinými výjimkami, protože programy **strmqikm** a **runmqckm** jsou na těchto platformách 32bitové.

Pomocí příkazu **runmqakm** :

```
-cert -import -file filename -pw password -type pkcs12
-crypto module_name -tokenlabel token_label -pw  password
-secondaryDB filename -secondaryDBpw password -fips
```

-cert -seznam
Seznam všech certifikátů na šifrovacím zařízení:

Pomocí příkazu **runmqckm** :

```
-cert -list all | personal | CA -crypto module_name
-tokenlabel token_label -pw  password
```

Používáte-li certifikáty nebo klíče uložené na šifrovacím hardwaru PKCS#11 , mějte na paměti, že **runmqckm** a **strmqikm** jsou 64bitové programy. Externí moduly požadované pro podporu PKCS#11 budou načteny do 64bitového procesu, proto musíte mít nainstalovanou 64bitovou knihovnu PKCS#11 pro administraci šifrovacího hardwaru. 32bitové platformy Windows a Linux x86 jsou jedinými výjimkami, protože programy **strmqikm** a **runmqckm** jsou na těchto platformách 32bitové.

Pomocí příkazu **runmqakm** :

```
-cert -list all | personal | CA -crypto module_name
-tokenlabel token_label -pw  password -fips
```

-cert -příjem
Přijmout certifikát ze souboru na šifrovací zařízení s podporou sekundární databáze klíčů:

Pomocí příkazu **runmqckm** :

```
-cert -receive -file filename -crypto module_name -tokenlabel  token_label
-pw password -default_cert yes | no -secondaryDB filename
-secondaryDBpw password -format  ascii | binary
```

Používáte-li certifikáty nebo klíče uložené na šifrovacím hardwaru PKCS#11 , mějte na paměti, že **runmqckm** a **strmqikm** jsou 64bitové programy. Externí moduly požadované pro podporu PKCS#11 budou načteny do 64bitového procesu, proto musíte mít nainstalovanou 64bitovou knihovnu PKCS#11 pro administraci šifrovacího hardwaru. 32bitové platformy Windows a Linux x86 jsou jedinými výjimkami, protože programy **strmqikm** a **runmqckm** jsou na těchto platformách 32bitové.

Pomocí příkazu **runmqakm** :

```
-cert -receive -file filename -crypto module_name -tokenlabel  token_label
-pw password -default_cert yes | no -secondaryDB filename
-secondaryDBpw password -format  ascii | binary -fips
```

-certreq -vytvořit
Vytvořte žádost o certifikát na šifrovacím zařízení:

Pomocí příkazu **runmqckm** :

```
-certreq -create -crypto module_name -tokenlabel token_label
-pw password -label label -dn distinguished_name
-size 1024 | 512 -file filename
-sig_alg MD2_WITH_RSA | MD2WithRSA | MD5_WITH_RSA |
MD5WithRSA | SHA1WithDSA | SHA1WithRSA |
SHA256_WITH_RSA | SHA256WithRSA |
SHA2WithRSA | SHA384_WITH_RSA |
SHA384WithRSA | SHA512_WITH_RSA |
SHA512WithRSA | SHA_WITH_DSA |
SHA_WITH_RSA | SHAWithDSA |
SHAWithRSA
```

Používáte-li certifikáty nebo klíče uložené na šifrovacím hardwaru PKCS#11 , mějte na paměti, že **runmqckm** a **strmqikm** jsou 64bitové programy. Externí moduly požadované pro podporu PKCS#11 budou načteny do 64bitového procesu, proto musíte mít nainstalovanou 64bitovou knihovnu PKCS#11 pro administraci šifrovacího hardwaru. 32bitové platformy Windows a Linux x86 jsou jedinými výjimkami, protože programy **strmqikm** a **runmqckm** jsou na těchto platformách 32bitové.

Pomocí příkazu **runmqakm** :

```
-certreq -create -crypto module_name -tokenlabel token_label
-pw password -label label -dn distinguished_name
-size 2048 | 1024 | 512 -file filename -fips
-sig_alg md5 | MD5_WITH_RSA | SHA_WITH_DSA |
SHA_WITH_RA | sha1 | SHA1WithDSA |
SHA1WithECDSA | SHA1WithRSA |
sha224 | SHA224_WITH_RSA | SHA224WithDSA |
SHA224WithECDSA | SHA224WithRSA |
sha256 | SHA256_WITH_RSA | SHA256WithDSA |
SHA256WithECDSA | SHA256WithRSA |
SHA2WithRSA | sha384 | SHA384_WITH_RSA |
SHA384WithECDSA | SHA384WithRSA |
sha512 | SHA512_WITH_RSA |
SHA512WithECDSA | SHA512WithRSA |
SHAWithDSA | SHAWithRSA |
EC_ecdsa_with_SHA1 | EC_ecdsa_with_SHA224 |
EC_ecdsa_with_SHA256 | EC_ecdsa_with_SHA384 |
EC_ecdsa_with_SHA512
```

-certreq -odstranění
Odstranit žádost o certifikát z šifrovacího zařízení:

Pomocí příkazu **runmqckm** :

```
-certreq -delete -crypto module_name -tokenlabel token_label
-pw password -label label
```

Používáte-li certifikáty nebo klíče uložené na šifrovacím hardwaru PKCS#11 , mějte na paměti, že **runmqckm** a **strmqikm** jsou 64bitové programy. Externí moduly požadované pro podporu PKCS#11 budou načteny do 64bitového procesu, proto musíte mít nainstalovanou 64bitovou knihovnu PKCS#11 pro administraci šifrovacího hardwaru. 32bitové platformy Windows a Linux x86 jsou jedinými výjimkami, protože programy **strmqikm** a **runmqckm** jsou na těchto platformách 32bitové.

Pomocí příkazu **runmqakm** :

```
-certreq -delete -crypto module_name -tokenlabel token_label
-pw password -label label -fips
```

-certreq -podrobnosti
Seznam podrobných informací o specifické žádosti o certifikát na šifrovacím zařízení:

Pomocí příkazu **runmqckm** :

```
-certreq -details -crypto module_name -tokenlabel token_label
-pw password -label label
```

Používáte-li certifikáty nebo klíče uložené na šifrovacím hardwaru PKCS#11 , mějte na paměti, že **runmqckm** a **strmqikm** jsou 64bitové programy. Externí moduly požadované pro podporu PKCS#11 budou načteny do 64bitového procesu, proto musíte mít nainstalovanou 64bitovou knihovnu PKCS#11 pro administraci šifrovacího hardwaru. 32bitové platformy Windows a Linux x86 jsou jedinými výjimkami, protože programy **strmqikm** a **runmqckm** jsou na těchto platformách 32bitové.

Pomocí příkazu **runmqakm** :

```
-certreq -details -crypto module_name -tokenlabel token_label
-pw password -label label -fips
```

Vypište podrobné informace o žádosti o certifikát a zobrazte úplnou žádost o certifikát na šifrovacím zařízení:

Pomocí příkazu **runmqckm** :

```
-certreq -details -showOID -crypto module_name -tokenlabel  token_label
-pw password -label label
```

Používáte-li certifikáty nebo klíče uložené na šifrovacím hardwaru PKCS#11 , mějte na paměti, že **runmqckm** a **strmqikm** jsou 64bitové programy. Externí moduly požadované pro podporu PKCS#11 budou načteny do 64bitového procesu, proto musíte mít nainstalovanou 64bitovou knihovnu PKCS#11 pro administraci šifrovacího hardwaru. 32bitové platformy Windows a Linux x86 jsou jedinými výjimkami, protože programy **strmqikm** a **runmqckm** jsou na těchto platformách 32bitové.

Pomocí příkazu **runmqakm** :

```
-certreq -details -showOID -crypto module_name -tokenlabel  token_label
-pw password -label label -fips
```

-certreq -extrakt
Extrahujte žádost o certifikát z databáze žádostí o certifikát na šifrovacím zařízení do souboru:

Pomocí příkazu **runmqckm** :

```
-certreq -extract -crypto module_name -tokenlabel token_label
-pw password -label label -target filename
```

Používáte-li certifikáty nebo klíče uložené na šifrovacím hardwaru PKCS#11 , mějte na paměti, že **runmqckm** a **strmqikm** jsou 64bitové programy. Externí moduly požadované pro podporu PKCS#11 budou načteny do 64bitového procesu, proto musíte mít nainstalovanou 64bitovou knihovnu PKCS#11 pro administraci šifrovacího hardwaru. 32bitové platformy Windows a Linux x86 jsou jedinými výjimkami, protože programy **strmqikm** a **runmqckm** jsou na těchto platformách 32bitové.

Pomocí příkazu **runmqakm** :

```
-certreq -extract -crypto module_name -tokenlabel token_label
-pw password -label label -target filename -fips
```

-certreq -seznam
Seznam všech žádostí o certifikát v databázi žádostí o certifikát na šifrovacím zařízení:

Pomocí příkazu **runmqckm** :

```
-certreq -list -crypto module_name -tokenlabel token_label
-pw password
```

Používáte-li certifikáty nebo klíče uložené na šifrovacím hardwaru PKCS#11 , mějte na paměti, že **runmqckm** a **strmqikm** jsou 64bitové programy. Externí moduly požadované pro podporu PKCS#11 budou načteny do 64bitového procesu, proto musíte mít nainstalovanou 64bitovou knihovnu PKCS#11 pro administraci šifrovacího hardwaru. 32bitové platformy Windows a Linux x86 jsou jedinými výjimkami, protože programy **strmqikm** a **runmqckm** jsou na těchto platformách 32bitové.

Pomocí příkazu **runmqakm** :

```
-certreq -list -crypto module_name -tokenlabel token_label
-pw password -fips
```

ALW Volby runmqckm a runmqakm na systému AIX, Linux, and Windows

Ke správě klíčů, certifikátů a žádostí o certifikáty můžete použít volby příkazového řádku **runmqckm** a **runmqakm** . Produkt **runmqckm** poskytuje funkce podobné funkcím produktu **iKeycmd**a produkt **runmqakm** poskytuje funkce podobné funkcím produktu **gskitcapicmd**.

Poznámka: Produkt IBM MQ nepodporuje algoritmy SHA-3 nebo SHA-5 . Můžete použít názvy algoritmů digitálního podpisu SHA384WithRSA a SHA512WithRSA , protože oba algoritmy jsou členy řady SHA-2 .

Deprecated Názvy algoritmů digitálního podpisu SHA3WithRSA a SHA5WithRSA jsou zamítnuty, protože se jedná o zkrácenou formu SHA384WithRSA a SHA512WithRSA .

Význam volby může záviset na objektu a akci uvedené v příkazu.

*Tabulka 97. Volby, které lze použít s volbami **runmqckm** a **runmqakm***

Parametr	Popis
`-create`	Volba pro vytvoření databáze klíčů.
`-crypto`	Název modulu pro správu šifrovacího zařízení PKCS #11 . Hodnota za hodnotou **-crypto** je volitelná, pokud zadáte název modulu v souboru vlastností. Pokud používáte certifikáty nebo klíče uložené na šifrovacím hardwaru PKCS #11 , všimněte si, že **runmqckm** a **strmqikm** jsou spuštěny pomocí prostředí JVM (Java Virtual Machine) dodaného s instalací produktu IBM MQ . Externí moduly požadované pro podporu PKCS #11 budou načteny do procesu JVM, proto musíte mít nainstalovanou knihovnu PKCS #11 pro administraci šifrovacího hardwaru, který odpovídá bitovému prostředí JVM, a tuto knihovnu musíte zadat **runmqckm** nebo **strmqikm**.
-db	Úplný název cesty databáze klíčů.
-default_cert	Nastaví certifikát jako výchozí certifikát. Hodnota může být `yes` nebo `no`. Výchozí hodnota je `Ne`.
-dn	X.500 rozlišující název. Hodnota je řetězec uzavřený v uvozovkách, například `"CN=John Smith,O=IBM,OU=Test,C=GB"`. Všimněte si, že jsou požadovány pouze atributy O a C. Určení obecného názvu (CN) je volitelné.
-encryption	Síla šifrování použitá v příkazu exportu certifikátu. Hodnota může být `silný` nebo `slabý`. Výchozí hodnota je `strong`.

*Tabulka 97. Volby, které lze použít s volbami **runmqckm** a **runmqakm** (pokračování)*	
Parametr	**Popis**
-expire	Doba vypršení platnosti certifikátu nebo hesla databáze ve dnech. Výchozí hodnota je 365 dní pro heslo certifikátu. Pro heslo databáze není výchozí čas: použijte parametr **-expire** k explicitnímu nastavení času vypršení platnosti hesla databáze.
-file	Název souboru certifikátu nebo žádosti o certifikát.
-fips	určuje, že příkaz má být spuštěn v režimu FIPS. V režimu FIPS komponenta IBM Crypto for C (ICC) používá algoritmy, které byly ověřeny podle standardu FIPS 140-2. Pokud se komponenta ICC neinicializuje v režimu FIPS, příkaz **runmqakm** se nezdaří.
-format	Formát certifikátu. Hodnota může být `ascii` pro Base64_encoded ASCII nebo `binary` pro binární data DER. Výchozí hodnota: `ascii`.
-label	Označení připojené k certifikátu nebo žádosti o certifikát. Pokud je certifikát osobním certifikátem používaným k identifikaci klientské aplikace nebo správce front IBM MQ , musí popisek odpovídat nastavení popisku certifikátu IBM MQ (CERTLABL), další informace viz “Digitální štítky certifikátů, pochopení požadavků” na stránce 26.
-new_format	Nový formát databáze klíčů.
-new_label	Tato volba, která se používá v příkazu pro import certifikátu, umožňuje importovat certifikát s jiným popiskem, než je popisek, který měl ve zdrojové databázi klíčů. Pokud je certifikát osobním certifikátem používaným k identifikaci klientské aplikace nebo správce front IBM MQ , musí popisek odpovídat nastavení popisku certifikátu IBM MQ (CERTLABL), další informace viz “Digitální štítky certifikátů, pochopení požadavků” na stránce 26.
-new_pw	Nové heslo databáze.
-old_format	Starý formát databáze klíčů.
-pw	Heslo pro databázi klíčů nebo soubor PKCS #12 .
-secondaryDB	Název sekundární databáze klíčů pro operace zařízení PKCS #11 .
-secondaryDBpw	Heslo pro sekundární databázi klíčů pro operace zařízení PKCS #11 .

runmqakm
-secretKey
`-add`
`-create`
`-extrahovat`
	
	Přidejte tajný klíč.
	Vytvořit náhodný tajný klíč
	Extrahovat tajný klíč z databáze klíčů

runmqckm
-secKey
`-create`
`-list`
`-export`
	
	Vytvořte náhodný tajný klíč.
	Vypsat tajné klíče
	Exportovat tajné klíče

-showOID	Zobrazí úplný certifikát nebo žádost o certifikát.

*Tabulka 97. Volby, které lze použít s volbami **runmqckm** a **runmqakm** (pokračování)*	
Parametr	**Popis**
-sig_alg	Hašovací algoritmus použitý během vytváření žádosti o certifikát, certifikátu podepsaného držitelem nebo podpisu certifikátu. Tento hašovací algoritmus se používá k vytvoření podpisu přidruženého k nově vytvořenému certifikátu nebo žádosti o certifikát. Hodnota **runmqckm**může být MD2_WITH_RSA, MD2WithRSA, MD5_WITH_RSA, MD5WithRSA, SHA1WithDSA, SHA1WithECDSA, SHA1WithRSA, SHA2/ECDSA, SHA224WithECDSA, SHA256_WITH_RSA, SHA256WithECDSA, SHA256WithRSA, SHA2WithECDSA, SHA3/ECDSA, SHA384_WITH_RSA, SHA384WithECDSA, SHA384WithRSA, SHA3WithECDSA, SHA5/ECDSA, SHA512_WITH_RSA, SHA512WithECDSA, SHA512WithRSA, SHA5WithECDSA, SHA_WITH_DSA, SHA_WITH_RSA, SHAWithDSA, SHAWithRSA. Výchozí hodnota je SHA1WithRSA. Pro systém **runmqakm**může být hodnota md5, MD5_WITH_RSA, MD5WithRSA, SHA_WITH_DSA, SHA_WITH_RSA, sha1, SHA1WithDSA, SHA1WithECDSA, SHA1WithRSA, sha224, SHA224_WITH_RSA, SHA224WithDSA, SHA224WithECDSA, SHA224WithRSA, sha256, SHA256_WITH_RSA, SHA256WithDSA, SHA256WithECDSA, SHA256WithRSA, SHA2WithRSA, sha384, SHA384_WITH_RSA, SHA384WithECDSA, SHA384WithRSA, sha512, SHA512_WITH_RSA, SHA512WithECDSA, SHA512WithRSA, SHAWithDSA, SHAWithRSA, EC_ecdsa_with_SHA1, EC_ecdsa_with_SHA224, EC_ecdsa_with_SHA256, EC_ecdsa_with_SHA384nebo EC_ecdsa_with_SHA512. Výchozí hodnota je SHA1WithRSA.
-size	Velikost klíče. Pro parametr **runmqckm**může být hodnota 512, 1024 nebo 2048. Výchozí hodnota je 1024 bitů. Pro parametr **runmqakm**hodnota závisí na podpisového algoritmu: • Pro podpisové algoritmy RSA (výchozí algoritmus použitý, pokud není uveden žádný **-sig_alg**) může být hodnota 512, 1024, 2048 nebo 4096. Velikost klíče RSA 512 bitů není povolena, pokud je povolen parametr **-fips** . Výchozí velikost klíče RSA je 2048 bitů. • Pro algoritmy eliptické křivky může být hodnota 256, 384 nebo 512. Výchozí velikost klíče eliptické křivky závisí na podpisovém algoritmu. Pro SHA256je to 256; pro SHA384je to 384 a pro SHA512je to 512.
-stash	Uložte heslo databáze klíčů do souboru. Platí pouze pro databáze typu CMS a PKCS12. **Poznámka:** Parametr **-stash** je platný v příkazech **-keydb** -create, který sdělí **runmqckm**/**runmqakm** , aby vytvořil soubor pro dočasné ukládání obsahující heslo. Zadání příkazu `$ runmqakm -help` vypíše pouze parametry nápovědy vysoké úrovně.

*Tabulka 97. Volby, které lze použít s volbami **runmqckm** a **runmqakm** (pokračování)*	
Parametr	**Popis**
-stashed	Označuje, že heslo pro databázi klíčů nebo soubor PKCS #12 je v souboru pro dočasné ukládání. **Poznámka:** Volba **-stashed** je platná pro volání kromě příkazů **-keydb** -create. Pokud tuto volbu neuvedete, musíte zadat heslo pomocí **-pw**. Kromě toho se zobrazí podrobná nápověda ukazující **-stashed** pouze v případě, že příkaz instruujete, jaký druh akce provádíte.
-stashpw	Uložte heslo databáze klíčů do souboru. Platí pouze pro databáze typu CMS a PKCS12.
-target	Cílový soubor nebo databáze.
-target_pw	Heslo pro databázi klíčů, pokud **-target** uvádí databázi klíčů.
-target_type	Typ databáze určený operandem **-target** . Povolené hodnoty viz parametr **-type** .
-tokenLabel	Popisek šifrovacího zařízení PKCS #11 .
-trust	Stav důvěryhodnosti certifikátu CA. Hodnota může být `enable` nebo `disable`. Výchozí nastavení je `enable`.
-type	Typ databáze. Hodnota může být některá z následujících: • `cms` pro databázi klíčů CMS • `pkcs12` pro soubor PKCS #12 .
-x509version	Verze certifikátu X.509 , který se má vytvořit. Hodnota může být 1, 2 nebo 3. Výchozí hodnota je 3.

-rfc3339	Tento parametr použijte pro výstup data ve formátu RFC 3339 pro příkaz `runmqakm -cert -details` , který má následující formát:
	`Not Before : 2015-08-26T08:53:37Z`
	`Not After : 2016-08-26T08:53:37Z`
	Všimněte si, že parametr **-rfc3339** se musí objevit v příkazu po dalších parametrech:
	`runmqakm -cert -details -db exampleDB -stashed -label certficateLabel -rfc3339`

ALW Kódy chyb příkazu runmqakm v systému AIX, Linux, and Windows

Tabulka číselných kódů chyb vydaných produktem **runmqakm**a jejich význam.

Kód chyby	Chybová zpráva
0	Úspěch
1	Došlo k neznámé chybě
2	Vyskytla se chyba kódování/dekódování ASN.1 .
3	Došlo k chybě při inicializaci enkodéru/dekodéru ASN.1 .

Kód chyby	Chybová zpráva
4	Došlo k chybě kódování/dekódování ASN.1 kvůli indexu mimo rozsah nebo neexistujícímu volitelnému poli.
5	Došlo k chybě databáze.
6	Došlo k chybě při otevírání databázového souboru, zkontrolujte existenci souboru a oprávnění.
7	Při opětovném otevírání databázového souboru došlo k chybě.
8	Vytvoření databáze se nezdařilo.
9	Databáze již existuje.
10	Při odstraňování databázového souboru došlo k chybě.
11	Databázi nelze otevřít.
12	Při čtení databázového souboru došlo k chybě.
13	Při zápisu dat do databázového souboru došlo k chybě.
14	Došlo k chybě ověření platnosti databáze.
15	Byla zjištěna neplatná verze databáze.
16	Bylo zjištěno neplatné heslo databáze.
17	Byl zjištěn neplatný typ databázového souboru.
18	Určená databáze byla poškozena.
19	Bylo zadáno neplatné heslo nebo došlo k manipulaci s databází klíčů nebo k její poškození.
20	Došlo k chybě integrity položky klíče databáze.
21	V databázi již existuje duplicitní certifikát.
22	V databázi již existuje duplicitní klíč (ID záznamu).
23	Certifikát se stejným popiskem již v databázi klíčů existoval.
24	V databázi již existuje duplicitní klíč (podpis).
25	V databázi již existuje duplicitní klíč (nepodepsaný certifikát).
26	V databázi již existuje duplicitní klíč (vydavatel a sériové číslo).
27	V databázi již existuje duplicitní klíč (informace o veřejném klíči předmětu).
28	V databázi již existuje duplicitní klíč (nepodepsaný CRL).
29	Popisek byl použit v databázi.
30	Došlo k chybě šifrování hesla.

Kód chyby	Chybová zpráva
31	Došlo k chybě související s LDAP. (LDAP není tímto programem podporován)
32	Došlo k šifrovací chybě.
33	Došlo k chybě šifrování/dešifrování.
34	Byl nalezen neplatný šifrovací algoritmus.
35	Při podepisování dat došlo k chybě.
36	Při ověřování dat došlo k chybě.
37	Při výpočtu kódu digest dat došlo k chybě.
38	Byl nalezen neplatný šifrovací parametr.
39	Byl zjištěn nepodporovaný šifrovací algoritmus.
40	Zadaná velikost vstupu je větší než podporovaná velikost modulu.
41	Byla nalezena nepodporovaná velikost modulu.
42	Došlo k chybě ověření platnosti databáze.
43	Ověření záznamu klíče se nezdařilo.
44	Existuje duplicitní pole rozšíření.
45	Verze klíče je chybná.
46	Požadované pole rozšíření neexistuje.
47	Doba platnosti nezahrnuje dnes nebo nespadá do doby platnosti emitenta.
48	Doba platnosti nezahrnuje dnešek nebo nespadá do doby platnosti emitenta.
49	Při ověřování platnosti rozšíření použití soukromého klíče došlo k chybě.
50	Vydavatel klíče nebyl nalezen.
51	Chybí požadované rozšíření certifikátu.
52	Bylo nalezeno neplatné rozšíření základního omezení.
53	Ověření podpisu klíče se nezdařilo.
54	Kořenový klíč klíče není důvěryhodný.
55	Klíč byl odvolán.
56	Při ověřování platnosti rozšíření identifikátoru klíče oprávnění došlo k chybě.
57	Při ověřování platnosti rozšíření použití soukromého klíče došlo k chybě.
58	Při ověřování platnosti rozšíření alternativního názvu subjektu došlo k chybě.
59	Při ověřování platnosti rozšíření alternativního názvu vydavatele došlo k chybě.

Kód chyby	Chybová zpráva
60	Při ověřování platnosti rozšíření použití klíče došlo k chybě.
61	Bylo nalezeno neznámé kritické rozšíření.
62	Při ověřování platnosti položek dvojice klíčů došlo k chybě.
63	Při ověřování seznamu CRL došlo k chybě.
64	Došlo k chybě mutexu.
65	Byl nalezen neplatný parametr.
66	Byl zjištěn parametr s hodnotou null nebo chyba alokace paměti.
67	Počet nebo velikost je příliš velká nebo příliš malá.
68	Staré heslo je neplatné.
69	Nové heslo je neplatné.
70	Platnost hesla vypršela.
66	Došlo k chybě související s podprocesem.
72	Při vytváření podprocesů došlo k chybě.
73	Při čekání podprocesu na ukončení došlo k chybě.
74	Došlo k chybě I/O.
75	Došlo k chybě při načítání CMS.
76	Došlo k chybě související s hardwarem šifrování.
77	Rutina inicializace knihovny nebyla úspěšně volána.
78	Interní tabulka manipulátoru databáze je poškozena.
79	Došlo k chybě alokace paměti.
80	Byla nalezena nerozpoznaná volba.
81	Při získávání informací o čase došlo k chybě.
82	Došlo k chybě vytvoření mutexu.
72	Při otevírání katalogu zpráv došlo k chybě.
84	Při otevírání katalogu chybových zpráv došlo k chybě.
85	Byl nalezen název souboru s hodnotou Null.
86	Došlo k chybě při otevírání souborů, zkontrolujte existenci souboru a oprávnění.
87	Při otevírání souborů ke čtení došlo k chybě.
88	Při otevírání souborů pro zápis došlo k chybě.
89	Takový soubor neexistuje.

Kód chyby	Chybová zpráva
90	Soubor nelze otevřít kvůli jeho nastavení oprávnění.
91	Při zápisu dat do souborů došlo k chybě.
92	Při odstraňování souborů došlo k chybě.
93	Byla nalezena neplatná data Base64-encoded .
94	Byl nalezen neplatný typ zprávy Base64 .
95	Při kódování dat pomocí pravidla kódování Base64 došlo k chybě.
96	Došlo k chybě při dekódování dat Base64-encoded .
97	Při získávání značky rozlišujícího názvu došlo k chybě.
98	Povinné pole obecného názvu je prázdné.
99	Požadované pole názvu země nebo oblasti je prázdné.
100	Byl nalezen neplatný popisovač databáze.
101	Databáze klíčů neexistuje.
102	Databáze dvojice klíčů požadavku neexistuje.
103	Soubor hesel neexistuje.
104	Nové heslo je stejné jako staré.
105	V databázi klíčů nebyl nalezen žádný klíč.
106	Nebyl nalezen žádný klíč požadavku.
107	Nebyla nalezena žádná důvěryhodná certifikační autorita.
108	Pro certifikát nebyl nalezen žádný klíč požadavku.
109	V databázi klíčů není žádný soukromý klíč.
110	V databázi klíčů není žádný výchozí klíč.
111	V záznamu klíče není žádný soukromý klíč.
112	V záznamu klíče není žádný certifikát.
113	Neexistuje žádná položka CRL.
114	Byl nalezen neplatný název souboru databáze klíčů.
115	Byl nalezen neznámý typ soukromého klíče.
116	Byl nalezen neplatný vstup rozlišujícího názvu.
117	Nebyla nalezena žádná položka klíče, která má uvedený popisek klíče.
118	Seznam popisků klíčů byl poškozen.
119	Vstupní data nejsou platná data PKCS12 .

Kód chyby	Chybová zpráva
120	Heslo je neplatné nebo data PKCS12 byla poškozena nebo byla vytvořena s novější verzí produktu PKCS12 .
121	Byl nalezen neznámý typ exportu klíče.
122	Byl nalezen nepodporovaný šifrovací algoritmus založený na hesle.
123	Při převodu souboru klíčového řetězce do databáze klíčů CMS došlo k chybě.
124	Došlo k chybě při převodu databáze klíčů CMS do souboru klíčového řetězce.
125	Při vytváření certifikátu pro žádost o certifikát došlo k chybě.
126	Nelze sestavit úplný řetězec vydavatele.
127	Byla nalezena neplatná data WEBDB.
128	Neexistují žádná data pro zápis do souboru klíčového řetězce.
129	Počet dnů, který jste zadali, přesahuje povolené období platnosti.
130	Heslo je příliš krátké; musí obsahovat alespoň {0} znaků.
131	Heslo musí obsahovat alespoň jednu číselnou číslici.
132	Všechny znaky v hesle jsou buď abecední, nebo číselné znaky.
133	Byl uveden nerozpoznaný nebo nepodporovaný podpisový algoritmus.
134	Byl zjištěn neplatný typ databáze.
135	Určenou sekundární databázi klíčů používá jiné zařízení PKCS#11 .
136	Nebyla zadána žádná sekundární databáze klíčů.
137	Popisek na zařízení PKCS#11 neexistuje.
138	Heslo požadované pro přístup k zařízení PKCS#11 .
139	Pro přístup k zařízení PKCS#11 není vyžadováno heslo.
140	Nelze načíst šifrovací knihovnu.
141	PKCS#11 není pro tuto operaci podporován.
142	Operace na zařízení PKCS#11 se nezdařila.
143	Uživatel LDAP není platný uživatel. (LDAP není tímto programem podporován)
144	Uživatel LDAP není platný uživatel. (LDAP není tímto programem podporován)

Kód chyby	Chybová zpráva
145	Dotaz LDAP se nezdařil. (LDAP není tímto programem podporován)
146	Byl nalezen neplatný řetěz certifikátů.
147	Kořenový certifikát není důvěryhodný.
148	Byl zjištěn odvolaný certifikát.
149	Funkce šifrovacího objektu selhala.
150	Není k dispozici žádný zdroj dat seznamu odvolaných certifikátů.
151	Není k dispozici žádný šifrovací token.
152	Režim FIPS není k dispozici.
153	Došlo ke konfliktu s nastavením režimu FIPS.
154	Zadané heslo neodpovídá minimální požadované síle.
200	Během inicializace programu došlo k selhání.
201	Tokenizace argumentů předaných programu runmqakm se nezdařila.
202	Objekt identifikovaný v příkazu není rozpoznávaným objektem.
203	Předaná akce není známou akcí -keydb.
204	Předaná akce není známou akcí -cert.
205	Předaná akce není známou akcí -certreq.
206	Pro požadovaný příkaz chybí značka.
207	Hodnota předaná se značkou -version není rozpoznanou hodnotou.
208	Hodnota předaná se značkou -size není rozpoznanou hodnotou.
209	Hodnota předaná se značkou -dn není ve správném formátu.
210	Hodnota předaná se značkou -format není rozpoznanou hodnotou.
211	Při otevírání souboru došlo k chybě.
212	PKCS12 není v této fázi podporován.
213	Šifrovací token, pro který se pokoušíte změnit heslo, není chráněn heslem.
214	PKCS12 není v této fázi podporován.
215	Zadané heslo neodpovídá minimální požadované síle.
216	Režim FIPS není k dispozici.
217	Počet dnů, které jste zadali jako datum vypršení platnosti, je mimo povolený rozsah.

Kód chyby	Chybová zpráva
218	Odolnost hesla nesplňovala minimální požadavky.
219	V požadované databázi klíčů nebyl nalezen žádný výchozí certifikát.
220	Byl zjištěn neplatný stav důvěryhodnosti.
221	Byl zjištěn nepodporovaný podpisový algoritmus. V této fázi jsou podporovány pouze položky Deprecated MD5 a Deprecated SHA1 .
222	PCKS11 není pro tuto konkrétní operaci podporován.
223	Předaná akce není známá-náhodná akce.
224	Délka menší než nula není povolena.
225	Při použití značky -strong je minimální délka hesla 14 znaků.
226	Při použití značky -strong je maximální délka hesla 300 znaků.
227	Algoritmus MD5 není podporován v režimu FIPS.
228	Značka site není pro příkaz -cert -list podporována. Tento atribut je přidán pro zpětnou kompatibilitu a potenciální budoucí rozšíření.
229	Hodnota přidružená ke značce -ca nebyla rozpoznána. Hodnota musí být buď 'true', nebo 'false'.
230	Hodnota předaná se značkou -type není platná.
231	Hodnota předaná se značkou -expire je pod povoleným rozsahem.
232	Použitý nebo požadovaný šifrovací algoritmus není podporován.
233	Cíl již existuje.

Ochrana hesel v konfiguračních souborech komponenty IBM MQ

Chcete-li použít určité funkce produktu IBM MQ, je možné, že hesla budou muset být dodána buď přímo do produktu IBM MQ , nebo v konfiguračních souborech, které funkce čte. Od produktu IBM MQ 9.2.0je implementován systém ochrany hesla, který chrání hesla v těchto konfiguračních souborech.

Hesla v konfiguračních souborech musí být šifrována. Následující seznam vysvětluje obecnou terminologii, která se používá pro každou komponentu:

Počáteční klíč
Šifrovací klíč, který se používá k ochraně hesla.

Pro každou uvedenou komponentu zadejte jedinečný počáteční klíč, který se používá k ochraně hesel uložených v konfiguraci této komponenty. Stejný počáteční klíč musí být také zpřístupněn komponentě, aby bylo možné heslo dešifrovat.

Většina komponent vyžaduje, aby byl v souboru dodán počáteční klíč. Počáteční soubor s klíči musí:

- **Obsahuje jeden řádek s alespoň jedním znakem.**
- Být odpovídajícím způsobem chráněn pomocí oprávnění operačního systému.

Neexistují žádné požadavky týkající se délky počátečního klíče nebo znaků, které lze zadat. Pro odpovídající zabezpečení byste však měli zadat počáteční klíč dlouhý alespoň 16 znaků. Váš počáteční soubor s klíči může například obsahovat:

```
Th1sIs@n3Ncypt|onK$y
```

Výchozí počáteční klíč
Výchozí použitý šifrovací klíč, pokud při šifrování dat nezadáte počáteční klíč. Neměli byste však **používat** výchozí počáteční klíč, protože dostatečně nechrání šifrovaná data.

Řetězec prostého textu
Řetězec, který je šifrovaný, obvykle heslo.

Šifrovaný řetězec hesla
Řetězec, který obsahuje šifrované heslo ve formátu, který produkt IBM MQ chápe.

Důležité: Zašifrované řetězce hesel, které jste vygenerovali pro použití s jednou komponentou, nelze zkopírovat do konfiguračního souboru jiné komponenty pro použití. Každé heslo pro každou komponentu musí být chráněno pomocí obslužného programu specifického pro danou komponentu.

Podrobnosti o tom, jak chránit hesla pro každou komponentu produktu IBM MQ , která podporuje ochranu heslem, jsou uvedeny v následujících sekcích:

- Advanced Message Security
- “Managed File Transfer” na stránce 582
- “IBM MQ Internet Pass-Thru” na stránce 583
- Deprecated “IBM MQ Bridge to blockchain” na stránce 584
- Deprecated “IBM MQ Bridge to Salesforce” na stránce 584
- V 9.3.0 “IBM MQ clients , které používají kryptografický hardware” na stránce 585
- “IBM MQ správce front” na stránce 585
- V 9.3.0 “IBM MQ Aplikace klienta C” na stránce 586
- V 9.3.2 “Nativní konfigurace vysoké dostupnosti” na stránce 586
- V 9.3.4 “IBM MQ správce front (AuthToken sekce v souboru qm.ini)” na stránce 587

Advanced Message Security

Klienti Advanced Message Security (AMS) Java vyžadují přístup k úložišti klíčů, které obsahuje soukromé klíče pro ochranu zprávy.

V 9.3.0 Advanced Message Security (AMS) Klienti MQI nebo správci front, kteří jsou konfigurováni pro provádění zachycení MCA, mohou vyžadovat přístup k šifrovanému hardwaru PKCS#11 nebo k souborům PEM, které obsahují soukromé klíče pro ochranu zpráv.

Chcete-li získat přístup k těmto souborům, musíte zadat heslo v konfiguračním souboru AMS , který se nazývá `keystore.conf`. Použijte příkaz **runamscred** k ochraně citlivých informací obsažených v souboru `keystore.conf` . Například:

```
runamscred -f <keystore configuration file>
```

Příkaz **runamscred** chrání citlivé parametry v uvedeném souboru pomocí příznaku **-f** .

V 9.3.0 Do instalace produktu IBM MQ se přidají dva programy **runamscred** :

- Program MQI **runamscred** umístěný v adresáři `<IBM MQ installation root>/bin`
- Program Java **runamscred** umístěný v adresáři `<IBM MQ installation root>/java/bin`

Upozornění: Aby byla zajištěna kompatibilita,

1. V 9.3.0 Pomocí programu Java **runamscred** můžete chránit konfigurační soubory, které mají být použity s klienty produktu Java AMS , a pomocí programu MQI **runamscred** můžete chránit konfigurační soubory, které mají být použity s klienty MQI AMS .
2. Po spuštění příkazu **runamscred**ověřte, že jsou všechny nezbytné citlivé informace chráněny.
3. Zadejte chráněný soubor jako obvykle pro aplikace s povoleným produktem AMS .

Chcete-li přepsat nebo poskytnout počáteční soubor s klíči, který se má použít za běhu aplikací AMS , nebo když chráníte konfigurační soubor úložiště klíčů pomocí produktu **runamscred**, použijte jeden z následujících čtyř mechanizmů v pořadí podle priority:

1. **-sf** parametr (pouze**runamscred**)
2. **MQS_AMSCRED_KEYFILE** proměnná prostředí
3. Parametr **amscred.keyfile** v konfiguračním souboru keystore.conf
4. Výchozí počáteční soubor s klíči, pokud není uvedena žádná z předchozích voleb.

Upozornění: V 9.3.0 Nepoužívejte výchozí počáteční klíč.

Před produktem IBM MQ 9.2byl k ochraně hesel v konfiguračních souborech produktu AMS Java použit jiný systém ochrany hesel.

Standardně program **runamscred** chrání hesla pomocí nového systému. To znamená, že nové konfigurační soubory nejsou kompatibilní se staršími verzemi produktu AMS Java. Chcete-li chránit konfigurační soubory pomocí starého systému ochrany heslem, použijte příznak **-sp** *0* .

Managed File Transfer

Managed File Transfer (MFT) ukládá pověření nezbytná pro přístup ke správcům front nebo jiným prostředkům v několika souborech vlastností XML:

- MQMFTCredentials.xml -Pověření pro připojení k agentu, koordinaci a správcům front příkazů a hesla pro připojení k úložištům klíčů pro zabezpečenou komunikaci.
- ProtocolBridgeCredentials.xml -Pověření pro připojení k serverům protokolu, například FTP/SFTP/FTPS.
- ConnectDirectCredentials.xml -Pověření pro agenta Connect:Direct pro připojení k uzlu Connect:Direct .

Další informace viz téma “Šifrování uložených pověření v adresáři MFT” na stránce 590.

Chcete-li chránit citlivé informace uložené v těchto souborech, použijte příkaz fteObfuscate v uvedeném souboru pomocí příznaku **-f** , například:

```
fteObfuscate -f <File to protect>
```

Chcete-li poskytnout počáteční soubor s klíči, který se má použít během ochrany konfigurací produktu MFT , použijte příznak **-sf** :

```
fteObfuscate -f <File to protect> -sf <initial key file>
```

Pokud nezadáte počáteční klíč, použije se k ochraně citlivých informací výchozí klíč, ačkoli byste tuto volbu neměli používat.

Upozornění:

1. Po spuštění příkazu **fteObfuscate**ověřte, že jsou všechny nezbytné citlivé informace chráněny.
2. Dodejte chráněný soubor jako obvykle do MFT.

Za běhu poskytněte počáteční soubor s klíči, který má být použit, prostřednictvím následujících tří mechanismů v pořadí podle priority:

1. Pomocí systémové vlastnosti Java .
   - V 9.3.1 V 9.3.0.10 Před IBM MQ 9.3.1 a IBM MQ 9.3.0 Fix Pack 10byl název této systémové vlastnosti Java chybně zapsán v kódu produktu jako `com.ibm.wqmfte.cred.keyfile`. V názvech IBM MQ 9.3.1 a IBM MQ 9.3.0 Fix Pack 10je pravopis názvu vlastnosti opraven na `com.ibm.wmqfte.cred.keyfile`. Produkt Managed File Transfer používá obě verze systémové vlastnosti Java , když kontroluje, zda uživatel uvedl soubor, který obsahuje počáteční klíč, který se má použít pro šifrování a dešifrování pověření. To umožňuje použít správný pravopis názvu vlastnosti při zachování kompatibility s dřívější verzí se starým chybně zadaným názvem. Všimněte si, že pokud jsou nastaveny obě systémové vlastnosti Java , použije se hodnota správně napsané vlastnosti `com.ibm.wmqfte.cred.keyfile` .
   - Před IBM MQ 9.3.1 a IBM MQ 9.3.0 Fix Pack 10použijte vlastnost `com.ibm.wqmfte.cred.keyfile`.
2. V souborech vlastností agenta, modulu protokolování, příkazů a koordinace.
3. V souboru `installation.properties` .

Před produktem IBM MQ 9.2byl k ochraně pověření v konfiguračních souborech MFT použit jiný systém ochrany pověření.

Standardně produkt **fteObfuscate** chrání pověření pomocí nového systému; to znamená, že konfigurační soubory nejsou kompatibilní se staršími verzemi produktu MFT.

Chcete-li chránit konfigurační soubory pomocí starého systému ochrany pověření, použijte parametr **-sp** *0* .

IBM MQ Internet Pass-Thru

Konfigurační soubor IBM MQ Internet Pass-Thru (MQIPT) může obsahovat hesla pro přístup k různým prostředkům a heslo pro administraci produktu MQIPT .

Tato hesla můžete chránit pomocí příkazu **mqiptPW** , který je dodáván s produktem MQIPT.

```
mqiptPW
```

Chcete-li chránit heslo se specifickým počátečním klíčem, zadejte příznak **-sf** :

```
mqiptPW -sf <intial key file>
```

Další informace viz Zadání šifrovacího klíče hesla.

Pokud nezadáte počáteční klíč, použije se k ochraně citlivých informací výchozí klíč, ačkoli byste tuto volbu neměli používat.

Produkt **mqiptPW** vás vyzve k bezpečnému zadání hesla pro ochranu a vrátí řetězec, který je třeba zkopírovat do konfiguračního souboru MQIPT .

Za běhu poskytněte počáteční soubor s klíči, který má být použit, prostřednictvím následujících čtyř mechanismů. V pořadí podle priority se jedná o:

1. Pomocí parametru **-sf** při spuštění MQIPT .
2. V proměnné prostředí MQS_MQIPTCRED_KEYFILE.
3. Ve vlastnosti **com.ibm.mq.ipt.cred.keyfile** Java .
4. V souboru s názvem `mqipt_cred.key` v domovském adresáři MQIPT se jedná o adresář, který obsahuje konfigurační soubory a soubory protokolu MQIPT a další.

Před produktem IBM MQ 9.2byl k ochraně pověření v konfiguračních souborech MQIPT použit jiný systém ochrany pověření.

Standardně produkt **mqiptPW** chrání pověření, která používají nový systém; to znamená, že konfigurační soubory nejsou kompatibilní se staršími verzemi produktu MQIPT.

Chcete-li chránit hesla úložiště klíčů, která používají starý systém ochrany pověření, použijte syntaxi příkazu **mqiptPW** , která je podporována ve verzích starších než IBM MQ 9.2.

IBM MQ Bridge to blockchain

Deprecated

Konfigurace produktu Bridge to blockchain jsou uloženy v souborech, které lze generovat pomocí příkazu **runmqbcb** . Při spuštění tohoto příkazu budete vyzváni k bezpečnému zadání hesel a umístění počátečního souboru s klíči, který se má použít.

Chcete-li přepsat počáteční soubor s klíči, který se má použít během běhového prostředí nebo režimu konfigurace, použijte příznak **-sf** . Například vygenerujte konfiguraci se specifickým počátečním souborem s klíči:

```
runmqbcb -o <output file> -sf <initial key file>
```

Nebo chcete-li použít specifický počáteční soubor s klíči za běhu:

```
runmqbcb -f <config file> -sf <initial key file>
```

Před produktem IBM MQ 9.2byl k ochraně pověření v konfiguračních souborech Bridge to blockchain použit jiný systém ochrany pověření.

Standardně produkt **runmqbcb** chrání pověření pomocí nového systému, což znamená, že konfigurační soubory nejsou kompatibilní se staršími verzemi produktu Bridge to blockchain.

Chcete-li chránit konfigurační soubory pomocí starého systému ochrany pověření, použijte příznak **-sp** *0* .

Důležité:

- Deprecated Produkt IBM MQ Bridge to blockchain je zamítnutý ve všech vydáních z 22. listopadu 2022 (viz Oznamovací dopis USA 222-341). Blockchain konektivitu lze dosáhnout pomocí funkcí IBM App Connect nebo App Connect , které jsou k dispozici s produktem IBM Cloud Pak for Integration.
- Pro Continuous Deliveryse IBM MQ Bridge to blockchain odebere z produktu na adrese IBM MQ 9.3.2.

IBM MQ Bridge to Salesforce

Deprecated

Konfigurace produktu Bridge to Salesforce jsou uloženy v souborech, které lze generovat pomocí příkazu **runmqsfb** . Při spuštění tohoto příkazu budete vyzváni k bezpečnému zadání hesel a umístění počátečního souboru s klíči, který se má použít.

Chcete-li přepsat počáteční soubor s klíči, který se má použít během běhového prostředí nebo režimu konfigurace, použijte příznak **-sf** . Chcete-li například vygenerovat konfiguraci se specifickým počátečním souborem s klíči, postupujte takto:

```
runmqsfb -o <output file> -sf <initial key file>
```

Nebo chcete-li použít specifický počáteční soubor s klíči za běhu:

```
runmqsfb -f <config file> -sf <initial key file>
```

Před produktem IBM MQ 9.2byl k ochraně pověření v konfiguračních souborech Bridge to Salesforce použit jiný systém ochrany pověření.

Standardně produkt **runmqfsb** chrání pověření pomocí nového systému, což znamená, že konfigurační soubory nejsou kompatibilní se staršími verzemi produktu Bridge to Salesforce.

Chcete-li chránit konfigurační soubory pomocí starého systému ochrany pověření, použijte příznak **-sp** *0* .

Důležité: Produkt IBM MQ Bridge to Salesforce je zamítnutý ve všech verzích od 22. listopadu 2022 (viz Oznamovací dopis USA 222-341).

IBM MQ clients , které používají kryptografický hardware

V 9.3.0

Klienty IBM MQ můžete nakonfigurovat tak, aby používali kryptografický hardware PKCS #11 k ukládání soukromých klíčů a certifikátů, které se používají v komunikaci TLS. Chcete-li přistupovat k zařízením PKCS #11 , musíte zadat heslo jako součást konfiguračního řetězce, který je dodán do produktu IBM MQ client.

Důležité: Hesla dodaná pomocí pole **CryptoHardware** ve struktuře MQCSO nebo pomocí tohoto mechanizmu nelze chránit atribut **SSLCRYP** správce front.

Toto heslo můžete chránit pomocí příkazu **runp11cred** , který najdete ve složce `bin` v instalačním adresáři IBM MQ .

Příkaz **runp11cred** vyzve k zadání hesla, které má být zašifrováno, a vrátí zašifrované heslo. Zašifrované heslo musí být zkopírováno do konfiguračního řetězce šifrovacího hardwaru.

Pokud je například konfigurační řetězec kryptografického hardwaru následující:

```
GSK_PKCS11=/usr/lib/pkcs11/PKCS11_API.so;tokenlabel;Passw0rd;SYMMETRIC_CIPHER_ON
```

Když vás příkaz **runp11cred** vyzve k zadání hesla, zadejte `Passw0rd`. Příkaz vrátí řetězec, který je podobný následujícímu:

```
<P11>!2!0TyDxrRaS6JUsjON9zfK6S4wEHmSNF0/ZsOdCaTD2dc=!MdpCoxGnFqPtZ1dTLQ58kg==
```

Nahraďte heslo v řetězci konfigurace šifrovacího hardwaru řetězcem, který je vrácen příkazem **runp11cred** , abyste poskytli následující řetězec, který obsahuje zašifrované heslo:

```
GSK_PKCS11=/usr/lib/pkcs11/PKCS11_API.so;tokenlabel;<P11>!2!0TyDxrRaS6JUsjON9zfK6S4wEHm SNF0/
ZsOdCaTD2dc=!MdpCoxGnFqPtZ1dTLQ58kg==;SYMMETRIC_CIPHER_ON
```

Uložte řetězec konfigurace šifrovacího hardwaru, který obsahuje šifrované heslo, buď v atributu **SSLCryptoHardware** v sekci SSL konfiguračního souboru klienta, nebo v proměnné prostředí **MQSSLCRYP** .

Standardně příkaz **runp11cred** zašifruje heslo pomocí výchozího počátečního klíče. Chcete-li chránit heslo vlastním počátečním klíčem, uveďte název souboru, který obsahuje počáteční klíč, pomocí jednoho z následujících mechanismů v pořadí podle priority:

1. Parametr **-sf** příkazu **runp11cred** .
2. Proměnná prostředí **MQS_SSLCRYP_KEYFILE** .

POZOR: K šifrování hesel nepoužívejte výchozí počáteční klíč, protože hesla nejsou bezpečně chráněna.

Pokud je při zašifrování hesla uveden počáteční soubor s klíči, musíte také uvést název souboru, který obsahuje počáteční klíč při spuštění produktu IBM MQ client . Zadejte počáteční název souboru s klíči pomocí jednoho z následujících mechanizmů v pořadí podle priority:

1. Proměnná prostředí **MQS_SSLCRYP_KEYFILE** .
2. Atribut **SSLCryptoHardwareKeyFile** v sekci **SSL** konfiguračního souboru klienta.

IBM MQ správce front

Správce front IBM MQ ukládá hesla interně do různých atributů, například do pole správce front **KEYRPWD** . Produkt IBM MQ automaticky zašifruje heslo před jeho uložením do souborů na disk.

Heslo úložiště klíčů může být chráněno buď pomocí systému ochrany hesla IBM MQ , nebo pomocí souboru pro dočasné ukládání úložiště klíčů. Další informace o těchto dvou metodách viz “Šifrování hesel úložiště klíčů v systému AIX, Linux, and Windows” na stránce 298.

Když správce front zašifruje heslo, použije se výchozí počáteční klíč, pokud není uveden alternativní klíč pomocí atributu **INITKEY** v objektu správce front. Před zadáním hesel, která mají být šifrována, nastavte jedinečný, silný klíč.

Upozornění: Úprava počátečního klíče po zadání přístupové fráze úložiště klíčů nezpůsobí zašifrování přístupové fráze úložiště klíčů pomocí nového počátečního klíče. Změna počátečního klíče bez opětovného zadání přístupové fráze úložiště klíčů má za následek, že produkt IBM MQ nemůže dešifrovat přístupovou frázi úložiště klíčů, a proto nemůže přistupovat k úložišti klíčů.

Další informace viz INITKEY.

IBM MQ Aplikace klienta C

V 9.3.0

Knihovny klienta IBM MQ C vyžadují hesla pro přístup k určitým zabezpečeným prostředkům, například úložiště klíčů TLS pro aplikace, které používají TLS pro připojení ke správci front.

Heslo úložiště klíčů může být chráněno buď pomocí systému ochrany hesla IBM MQ , nebo pomocí souboru pro dočasné ukládání úložiště klíčů. Další informace o těchto dvou metodách viz “Šifrování hesel úložiště klíčů v systému AIX, Linux, and Windows” na stránce 298.

Chcete-li chránit hesla pomocí systému ochrany hesel IBM MQ , použijte příkaz **runmqicred** . Příkaz je umístěn v adresáři *MQ_INSTALLATION_PATH*/bin .

Příkaz **runmqicred** vyzve k zadání hesla, které má být zašifrováno, a vrátí zašifrované heslo, které lze použít místo hesla v prostém textu.

Pokud se například rozhodnete zadat heslo úložiště klíčů TLS pomocí proměnné prostředí *MQKEYRPWD* a vaše heslo úložiště klíčů TLS je Passw0rd. Když spustíte příkaz **runmqicred**, zadejte na výzvu Passw0rd . Příkaz vrátí řetězec, který je podobný následujícímu:

```
<MQI>!2!G4lRxBuiNfJ3uOeYTD3lG1hrL5NvVZLAlgZCX3Tn6d8=!pUDOErDfDi9+JFVa0usS7w==
```

Nastavte tento řetězec jako hodnotu proměnné prostředí *MQKEYRPWD* :

```
export MQKEYRPWD="<MQI>!2!G4lRxBuiNfJ3uOeYTD3lG1hrL5NvVZLAlgZCX3Tn6d8=!pUDOErDfDi9+JFVa0usS7w=="
set MQKEYRPWD="<MQI>!2!G4lRxBuiNfJ3uOeYTD3lG1hrL5NvVZLAlgZCX3Tn6d8=!pUDOErDfDi9+JFVa0usS7w=="
```

Standardně příkaz **runmqicred** zašifruje heslo pomocí výchozího počátečního klíče. Chcete-li chránit heslo pomocí vlastního počátečního klíče, použijte jeden z následujících mechanismů k určení názvu souboru, který obsahuje klíč, v pořadí podle priority:

1. Parametr **-sf** příkazu **runmqicred** .
2. Proměnná prostředí **MQS_MQI_KEYFILE** .

POZOR: K šifrování hesel nepoužívejte výchozí počáteční klíč, protože hesla nejsou bezpečně chráněna.

Další informace viz téma “Zadání hesla úložiště klíčů pro IBM MQ MQI client on AIX, Linux, and Windows” na stránce 304.

Nativní konfigurace vysoké dostupnosti

V 9.3.2

Přenos replikace nativního protokolu HA mezi instancemi lze šifrovat pomocí TLS. Certifikáty, které se používají k zabezpečení provozu replikace protokolu, jsou uloženy v úložišti klíčů, které je uvedeno v sekci **NativeHALocalInstance** souboru qm.ini .

Heslo úložiště klíčů může být chráněno buď pomocí systému ochrany hesla IBM MQ , nebo pomocí souboru pro dočasné ukládání úložiště klíčů. Další informace o těchto dvou metodách viz “Šifrování hesel úložiště klíčů v systému AIX, Linux, and Windows” na stránce 298.

Chcete-li chránit heslo úložiště klíčů nativní vysoké dostupnosti pomocí systému ochrany hesla IBM MQ , použijte příkaz **runmqicred** .

Příkaz **runmqicred** vyzve k zadání hesla, které má být zašifrováno, a vrátí zašifrované heslo, které by mělo být použito místo hesla v prostém textu. Nastavte hodnotu atributu **KeyRepositoryPassword** v sekci **NativeHALocalInstance** souboru `qm.ini` na zašifrované heslo vrácené příkazem.

Standardně příkaz **runmqicred** zašifruje heslo pomocí výchozího počátečního klíče. Chcete-li chránit heslo pomocí vlastního počátečního klíče, použijte jeden z následujících mechanismů k určení názvu souboru, který obsahuje klíč, v pořadí podle priority:

1. Parametr **-sf** příkazu **runmqicred** .
2. Proměnná prostředí *MQS_MQI_KEYFILE* .

POZOR: K šifrování hesel nepoužívejte výchozí počáteční klíč, protože hesla nejsou bezpečně chráněna.

Pokud zašifrujete heslo úložiště klíčů svým vlastním počátečním klíčem, musíte také uvést stejný počáteční soubor s klíči pomocí atributu **InitialKeyFile** v sekci **NativeHALocalInstance** souboru `qm.ini` .

Další informace viz NativeHALocalSekce instance souboru qm.ini.

IBM MQ správce front (AuthToken sekce v souboru `qm.ini`)

Linux V 9.3.4 AIX

V operačním systému IBM MQ 9.3.4může produkt IBM MQ MQI clients , který se připojuje ke správcům front systému IBM MQ spuštěným v systémech AIX nebo Linux , používat tokeny ověřování k ověřování u správce front. Správce front musí být konfigurován tak, aby přijímal tokeny ověřování a měl přístup k certifikátu veřejného klíče vydavatele tokenu nebo k tajnému klíči použitému k podepsání tokenu. Úložiště klíčů, které obsahuje certifikáty veřejného klíče důvěryhodného vydavatele nebo tajné klíče, je zabezpečeno heslem.

Heslo úložiště klíčů může být chráněno buď pomocí systému ochrany hesla IBM MQ , nebo pomocí souboru pro dočasné ukládání úložiště klíčů. Další informace o těchto dvou metodách viz “Šifrování hesel úložiště klíčů v systému AIX, Linux, and Windows” na stránce 298.

Chcete-li chránit heslo úložiště klíčů tokenu ověření pomocí systému ochrany hesla IBM MQ , použijte příkaz **runqmcred** k zašifrování hesla.

Chcete-li zašifrovat heslo pomocí specifického počátečního klíče, zadejte pomocí parametru **-sf** cestu k souboru, který obsahuje počáteční klíč. Pokud počáteční klíč nezadáte, použije se výchozí počáteční klíč.

POZOR: K šifrování hesel nepoužívejte výchozí počáteční klíč, protože hesla nejsou bezpečně chráněna.

Důležité: Pokud zadáte počáteční soubor s klíči, který obsahuje šifrovací klíč, musí být v atributu **INITKEY** správce front uveden stejný počáteční klíč, aby mohl správce front heslo dešifrovat. Pokud je atribut **INITKEY** správce front již nastaven, použijte při spuštění příkazu **runqmcred** stejný počáteční klíč. Další informace o atributu **INITKEY** správce front viz INITKEY.

Chcete-li například zašifrovat hesla úložiště klíčů tokenu ověření pomocí počátečního klíče v souboru `/home/initial.key`, zadejte následující příkaz:

```
runqmcred -sf /home/initial.key
```

Po zobrazení výzvy zadejte heslo, které chcete šifrovat.

```
5724-H72 (C) Copyright IBM Corp. 1994, 2024.
Enter password:
```

```
*************
<QM>!2!UnH/9hRXEGA0cenLVSGCW9a0s5A2vHDkTiA7vRv8ogc=!yhlsHFw7MIh48SvaYeTwRQ==
```

Šifrované heslo je výstupem na posledním řádku. Zkopírujte šifrované heslo do souboru a zahrňte cestu k souboru do atributu **KeyStorePwdFile** sekce **AuthToken** v souboru `qm.ini` .

Další informace viz téma “Konfigurace správce front pro přijetí tokenů ověřování” na stránce 353.

Omezení ochrany pomocí šifrování hesla

Produkt IBM MQ podporuje šifrování AES-128 pro hesla uložená v různých konfiguračních souborech. Když používáte šifrování AES (Advanced Encryption Standard) k ochraně hesel v konfiguraci IBM MQ , musíte porozumět omezením ochrany, kterou poskytuje.

Šifrování hesla v konfiguračních souborech IBM MQ neznamená, že je heslo zabezpečené nebo chráněné. To pouze brání tomu, aby heslo bylo snadno obnoveno někým, kdo má přístup k zašifrovanému heslu, ale nezná šifrovací klíč. Procesy IBM MQ vyžadují přístup jak k šifrovanému heslu, tak k dešifrovacímu klíči, aby získaly heslo v prostém textu, které se má použít. Obě tyto datové položky musí být uloženy v systému souborů v umístění, které je přístupné pro produkt IBM MQ. Každý, kdo zašifruje heslo umístěné v konfiguračním souboru, také vyžaduje přístup k šifrovacímu klíči. Pokud má útočník přístup ke stejné sadě souborů jako IBM MQ, použití šifrování AES na heslo poskytuje pouze minimální úroveň ochrany.

Nicméně šifrování hesel v klidu je důležité zvážit, protože zabraňuje náhodnému zveřejnění hesel a umožňuje sdílení konfiguračních souborů, pokud není dešifrovací klíč také sdílen.

Kromě zajištění, že soubor, který obsahuje dešifrovací klíč, není sdílený, je třeba dbát na to, aby byl soubor chráněn před ostatními uživateli v systému. Zatímco konfigurační soubory IBM MQ mohou být přístupné všem uživatelům, omezte oprávnění k souboru, který obsahuje dešifrovací klíč, na nezbytné minimum. ID uživatelů, která produkt IBM MQ zpracovává, musí mít udělen přístup pro čtení souboru, který obsahuje dešifrovací klíč. Není však nutné udělit přístup ke čtení souboru skupině nebo všem uživatelům v systému.

Ochrana podrobností ověření databáze

Pokud pro připojení ke správci databází používáte ověřování pomocí jména uživatele a hesla, můžete je uložit do úložiště pověření XA produktu MQ , abyste se vyvarovali ukládání hesla v prostém textu do souboru `qm.ini` .

Aktualizovat XAOpenString pro správce prostředků

Chcete-li použít úložiště pověření, musíte upravit XAOpenString v souboru `qm.ini` . Řetězec se používá pro připojení ke správci databází. Určujete nahraditelná pole, abyste identifikovali, kde je jméno uživatele a heslo nahrazeno v řetězci XAOpenString .

- Pole +USER+ je nahrazeno hodnotou jména uživatele uloženou v úložišti XACredentials.
- Pole +PASSWORD+ je nahrazeno hodnotou hesla uloženou v úložišti XACredentials.

Následující příklady ukazují, jak upravit XAOpenString pro použití souboru pověření pro připojení k databázi.

Připojení k databázi Db2

```
XAResourceManager:
  Name=mydb2
  SwitchFile=db2swit
  XAOpenString=db=mydbname,uid=+USER+,pwd=+PASSWORD+,toc=t
  ThreadOfControl=THREAD
```

Připojení k databázi Oracle

```
XAResourceManager:
  Name=myoracle
  SwitchFile=oraswit
```

```
XAOpenString=Oracle_XA+Acc=P/+USER+/+PASSWORD++SesTm=35
          +LogDir=/tmp+threads=true
ThreadOfControl=THREAD
```

Práce s pověřeními databáze pro úložiště pověření XA produktu MQ

Po aktualizaci souboru `qm.ini` pomocí nahraditelných řetězců pověření musíte přidat jméno uživatele a heslo do úložiště pověření produktu MQ pomocí příkazu **setmqxacred** . Pomocí produktu **setmqxacred** můžete také upravit existující pověření, odstranit pověření nebo vypsat pověření. Následující příklady uvádějí některé typické případy použití:

Přidání pověření

Následující příkaz bezpečně uloží jméno uživatele a heslo pro správce front `QM1` pro prostředek `mqdb2`.

```
setmqxacred -m QM1 -x mydb2 -u user1 -p Password2
```

Aktualizace pověření

Chcete-li aktualizovat jméno uživatele a heslo použité pro připojení k databázi, zadejte příkaz **setmqxacred** znovu s novým jménem uživatele a heslem:

```
setmqxacred -m QM1 -x mydb2 -u user3 -p Password4
```

Změny se projeví až po restartování správce front.

Odstranění pověření

Následující příkaz odstraní pověření:

```
setmqxacred -m QM1 -x mydb2 -d
```

Výpis pověření

Následující příkaz vypíše pověření:

```
setmqxacred -m QM1 -l
```

Související odkazy

setmqxacred

zabezpečeníManaged File Transfer

Přímo po instalaci a bez úprav má produkt Managed File Transfer úroveň zabezpečení, která může být vhodná pro účely testování nebo vyhodnocení v chráněném prostředí. V produkčním prostředí však musíte zvážit vhodné řízení toho, kdo může zahájit operace přenosu souborů, kdo může číst a zapisovat přenášené soubory a jak chránit integritu souborů.

Související úlohy

Omezení oprávnění skupiny pro prostředky specifické pro MFT

Správa oprávnění pro prostředky specifické pro systém MFT

“Použití Advanced Message Security s Managed File Transfer” na stránce 654

Tento scénář vysvětluje, jak nakonfigurovat produkt Advanced Message Security tak, aby poskytoval soukromí zpráv pro data odesílaná prostřednictvím produktu Managed File Transfer.

Související odkazy

Oprávnění pro MFT pro přístup k systémům souborů

Vlastnost commandPath MFT

Oprávnění k publikování zpráv protokolu a stavových zpráv agentů MFT

Šifrování uložených pověření v adresáři MFT

Managed File Transfer (MFT) vyžaduje několik ID uživatelů a pověření, která jsou uložena ve dvou souborech XML, a můžete je zamlžovat pomocí příkazu **fteObfuscate** . V systému IBM MQ 9.2.0tento příkaz poskytuje rozšířenou ochranu uložených pověření.

Soubory pověření

MQMFTCredentials.xml
Tento soubor obsahuje ID uživatele a pověření pro připojení k agentům a koordinaci a správce front příkazů. Pověření pro přístup k úložištím klíčů pro zabezpečená připojení ke správcům front jsou také uložena ve stejném souboru.

Podrobnosti o hodnotách vlastností, které definují umístění souboru `MQMFTCredentials.xml` , viz “Ověření připojení MFT a IBM MQ” na stránce 593 .

ProtocolBridgeCredentials.xml
Tento soubor obsahuje ID uživatele a pověření pro připojení k serverům protokolu.

Šifrování pověření pomocí příkazu `fteObfuscate`

V systému IBM MQ 9.2.0příkaz **fteObfuscate** přijímá následující parametry:

- **-f** *credentials_file_name* (povinné)

  Poznámka: Deprecated Tento parametr nahrazuje parametr **-credentialsFile** , který je zamítnutý z IBM MQ 9.2.0.
- **-sp** *režim_ochrany*
- **-sf** *soubor credentials_key_file*
- **-o** *název_výstupního_souboru*

Podrobnosti o parametrech viz **fteObfuscate** .

Pokud neuvedete režim ochrany nebo soubor s klíči pověření, příkaz použije výchozí režim ochrany a použije nejnovější algoritmus, ale s pevným klíčem k zašifrování pověření.

Pokud uvedete režim ochrany `0`a neuvedete soubor s klíči pověření, příkaz bude fungovat jako v předchozích vydáních produktu. Na konzole obdržíte varovnou zprávu označující použití zamítnuté ochrany.

Pokud uvedete režim ochrany `0`a uvedete soubor s klíči pověření, obdržíte na konzole chybový výstup označující, že není platné uvést soubor s klíči při použití režimu ochrany `0`.

Pokud uvedete režim ochrany 1a neuvedete soubor s klíči pověření, příkaz použije nejnovější algoritmus, ale s pevným klíčem k zašifrování pověření.

Pokud uvedete režim ochrany 1a uvedete soubor s klíči pověření, příkaz zašifruje pověření pomocí nejnovějšího algoritmu.

Pokud uvedete režim ochrany 1nebo neuvedete režim ochrany a uvedete soubor s klíči pověření, který neexistuje, na konzole se objeví chyba označující, že soubor neexistuje.

Pokud uvedete režim ochrany 1nebo neuvedete režim ochrany a uvedete soubor s klíči pověření, který není čitelný, na konzole se objeví chyba označující, že soubor není čitelný.

V 9.3.0 Pokud uvedete režim ochrany 2a neuvedete soubor s klíči pověření, příkaz použije režim ochrany 2 k zašifrování pověření pomocí nejnovějšího algoritmu a pevného klíče k zašifrování.

V 9.3.0 Pokud uvedete režim ochrany 2a uvedete soubor s klíči pověření, příkaz použije režim ochrany 2 k zašifrování pověření pomocí nejnovějšího algoritmu a uživatelem uvedeného klíče k zašifrování.

V 9.3.0 Pokud uvedete režim ochrany 2nebo neuvedete režim ochrany a uvedete soubor s klíči pověření, který neexistuje, na konzole se objeví chyba označující, že soubor neexistuje.

V 9.3.0 Pokud uvedete režim ochrany 2nebo neuvedete režim ochrany a uvedete soubor s klíči pověření, který není čitelný, na konzole se objeví chyba označující, že soubor není čitelný.

Dešifrování pověření

Cestu k počátečnímu souboru s klíči můžete zadat na různých místech. Chcete-li dešifrovat pověření, která byla zašifrována pomocí jiného než výchozího klíče, název souboru obsahujícího počáteční klíč musí být produktu MFT poskytnut jedním z následujících způsobů, v tomto pořadí:

1. Pomocí systémové vlastnosti Java , například:

   ```
   -Dcom.ibm.wmqfte.cred.keyfile=/usr/hime/credkeyfile.key
   ```

   Poznámka:

   - V 9.3.1 Před IBM MQ 9.3.1byl název této systémové vlastnosti Java chybně zapsán v kódu produktu jako `com.ibm.wqmfte.cred.keyfile`. V produktu IBM MQ 9.3.1je pravopis názvu vlastnosti opraven na hodnotu `com.ibm.wmqfte.cred.keyfile`. Produkt Managed File Transfer používá obě verze systémové vlastnosti Java při kontrole, zda uživatel zadal soubor obsahující počáteční klíč, který by měl být použit pro šifrování a dešifrování pověření. To vám umožňuje použít správný pravopis názvu vlastnosti při zachování zpětné kompatibility se starým chybně zadaným názvem. Všimněte si, že pokud jsou nastaveny obě systémové vlastnosti Java , použije se hodnota správně napsané vlastnosti `com.ibm.wmqfte.cred.keyfile` .
   - Před IBM MQ 9.3.1použijte vlastnost `com.ibm.wqmfte.cred.keyfile`.

   .
2. Nastavením vlastnosti v souboru vlastností agenta, příkazu, koordinace nebo modulu protokolování. Název souboru vlastností a vlastnost, kterou je třeba v něm nastavit, jsou uvedeny v následující tabulce:

soubor vlastností	**Název vlastnosti**
agent.properties	agentCredentialsKeyFile
command.properties	commandCredentialsKeyFile
coordination.properties	coordinationCredentialsKeyFile
logger.properties	loggerCredentialsKeyFile

3. V souboru installation.properties .

   Místo přidávání vlastností do jednotlivých souborů vlastností můžete přidat vlastnost **`commonCredentialsKeyFile`** do existujícího společného souboru `installation.properties` , aby agent, modul protokolování a příkazy mohly používat stejnou vlastnost.

Pokud jste definovali různé vlastnosti **`CredentialsKeyFile`** ve více umístěních:

- Cesta k souboru s klíči pověření, který se používá pro agenta a modul protokolování, se zaprotokoluje do souboru `output0.log` pro tohoto agenta nebo modul protokolování.
- Na konzole se zobrazí cesta k souboru s klíči pověření, který se používá pro příkazy.

Java Systémová vlastnost **`com.ibm.wmqfte.cred.keyfile`** přepíše všechny ostatní. Není-li systémová vlastnost nastavena, agent vyhledá soubor `agent.properties` následovaný souborem `installation.properties` pro počáteční soubor s klíči.

Pokud počáteční soubor s klíči stále není nalezen a vy jste nastavili režim ochrany v příkazu **`fteObfuscate`** na 1, agent zaprotokoluje chybovou zprávu do souboru `output0.log` .

Pokud jste nastavili režim ochrany na hodnotu 0 v příkazu **fteObfuscate** , zaprotokoluje se varovná zpráva označující zamítnutí.

Zapisovač protokolu a příkazy následují stejné kroky pro vyhledání počátečního souboru s klíči.

Most protokolů a most Connect:Direct

Most protokolů používá soubor vlastností `ProtocolBridgeProperties.xml`pro připojení k serverům FTP, SFTP a FTPS. Tento soubor vlastností obsahuje atributy připojení nezbytné pro připojení k těmto serverům.

Pokud upravíte hodnotu atributů **credentialsFile** nebo **credentialsKeyFile** v souboru `ProtocolBridgeProperties.xml` , je vyžadován restart agenta mostu.

Jeden z atributů je **credentialsFile**a hodnota obsahuje cestu k souboru XML, který obsahuje UID nebo PWD, nebo Klíč požadovaný pro připojení k těmto serverům. Výchozí hodnota atributu je *ProtocolBridgeCredentials.xml* a soubor je ve vašem domovském adresáři, stejně jako soubor `MQMFTCredentials.xml` .

```
<tns:credentialsFile path="$HOME/ProtocolBridgeCredentials.xml" />
```

Stejně jako *MQMFTCredentails.xml*můžete šifrovat *ProtocolBridgeCredentials.xml* pomocí příkazu **fteObfuscate** . Pro účely dešifrování můžete uvést požadovanou cestu k souboru s klíči pověření pomocí dalšího prvku **credentialsKeyFile** , jak je zobrazeno v následujícím textu. Cesta může obsahovat proměnné prostředí.

```
<tns:credentialsKeyFile path="$HOME/CredKey.key"/>
```

Poznámka: Uvedení hodnoty pro vlastnost **agentCredentialsKeyFile** agent, **commonCredentialsKeyFile** ve vlastnosti `installation.propertiesnebo` prostřednictvím systémové vlastnosti **com.ibm.wqmfte.cred.keyfile**nemá žádný vliv na hodnotu uvedenou pro atribut **credentialsKeyFile** .

Podobně produkt Connect:Direct Bridge používá soubor *ConnectDirectNodeProperties.xml* pro připojení k serveru Connect:Direct . Soubor XML obsahuje požadované informace o připojení spolu s atributem, který definuje cestu k souboru XML pověření. Tento soubor XML pověření obsahuje UID nebo PWD a další informace požadované pro připojení k serveru Connect:Direct .

```
<tns:credentialsFile path="$HOME/ ConnectDirectCredentials.xml" />
```

Stejně jako soubor *ProtocolBridgeCredentials.xml* můžete šifrovat soubor *ConnectDirectCredentials.xml* pomocí příkazu **fteObfuscate** . Pro účely dešifrování můžete uvést požadovanou cestu k souboru s klíči pověření pomocí dalšího prvku **credentialsKeyFile** , jak je zobrazeno v následujícím textu. Cesta může obsahovat proměnné prostředí.

```
<tns:credentialsKeyFile path="$HOME/CredKey.key"/>
```

Poznámka: Uvedení hodnoty pro vlastnost **agentCredentialsKeyFile** agent, **commonCredentialsKeyFile** ve vlastnosti `installation.propertiesnebo` prostřednictvím systémové vlastnosti **com.ibm.wqmfte.cred.keyfile** nemá žádný vliv na hodnotu uvedenou pro atribut **credentialsKeyFile** .

Prvek **credentialsKeyFile** můžete určit bez určení prvku **credentialsFile** v souboru *ProtocolBridgeProperties.xml* .

Pokud neuvedete prvek **credentialsFile** , agent mostu protokolů použije výchozí soubor pověření *ProtocolBridgeCredentials.xml* a hodnota souboru s klíči uvedená v atributu **credentialsKeyFile** se použije k dešifrování souboru pověření.

Podobně můžete určit prvek **credentialsKeyFile** bez určení prvku **credentialsFile** v souboru *ConnectDirectNodeProperties.xml* .

Pokud neuvedete prvek **credentialsFile** , most Connect:Direct použije výchozí soubor pověření *ConnectDirectCredentials.xml* a hodnota souboru s klíči uvedená v atributu **credentialsKeyFile** se použije k dešifrování souboru pověření.

Použití klíče z datové sady na systému z/OS

z/OS

V systému z/OSmůžete uvést **MQMFTCredentials** a poskytnout soubor s klíči pověření pomocí PDSE. Viz téma “Konfigurace MQMFTCredentials.xml na systému z/OS” na stránce 595.

Související odkazy

Který příkaz MFT se připojuje ke kterému správci front

Formát souboru pověření MFT

fteObfuscate (šifrovat citlivá data)

Ověření připojení MFT a IBM MQ

Ověřování připojení umožňuje konfigurovat správce front pro ověřování aplikací pomocí zadaného jména uživatele a hesla. Pokud má přidružený správce front povoleno zabezpečení a vyžaduje podrobnosti o pověření (ID uživatele a heslo), musí být před úspěšným připojením ke správci front povolena funkce ověřování připojení. Ověřování připojení lze spustit v režimu kompatibility nebo v režimu ověřování MQCSP.

Metody zadání podrobností pověření

Mnoho příkazů Managed File Transfer podporuje následující metody zadání podrobností pověření:

Podrobnosti poskytnuté argumenty příkazového řádku.
Podrobnosti pověření lze zadat pomocí parametrů **-mquserid** a **-mqpassword** . Není-li zadán parametr **-mqpassword** , bude uživatel požádán o zadání hesla, kde se vstup nezobrazí.

Podrobnosti poskytnuté ze souboru pověření: MQMFTCredentials.xml.
Podrobnosti pověření mohou být předdefinovány v souboru `MQMFTCredentials.xml` buď jako prostý text, nebo jako zamlovaný text.

Informace o nastavení souboru MQMFTCredentials.xml v tématu IBM MQ for Multiplatforms viz “Konfigurace souboru MQMFTCredentials.xml na platformě Multiplatforms” na stránce 594.

Informace o nastavení souboru MQMFTCredentials.xml v tématu IBM MQ for z/OS viz “Konfigurace MQMFTCredentials.xml na systému z/OS” na stránce 595.

Přednost

Priorita určení podrobností pověření je:

1. Argument příkazového řádku.
2. Index `MQMFTCredentials.xml` podle přidruženého správce front a uživatele, který spustil příkaz.
3. `MQMFTCredentials.xml` index podle přidruženého správce front.
4. Výchozí režim zpětné kompatibility, ve kterém nejsou zadány žádné podrobnosti pověření umožňující kompatibilitu s předchozími verzemi produktu IBM MQnebo IBM WebSphere MQ

Notes:

- Příkazy **fteStartAgent** a **fteStartLogger** nepodporují argument příkazového řádku **-mquserid**nebo **-mqpassword**a podrobnosti pověření lze zadat pouze se souborem `MQMFTCredentials.xml` .
- z/OS

  V systému z/OSmusí být heslo velké, i když má heslo uživatele malá písmena. Například, pokud bylo heslo uživatele "password", muselo by být zadáno jako "PASSWORD".

Související odkazy

Který příkaz MFT se připojuje ke kterému správci front

Formát souboru pověření MFT

Konfigurace souboru MQMFTCredentials.xml na platformě Multiplatforms

Je-li Managed File Transfer (MFT) nakonfigurován s povoleným zabezpečením, ověření připojení vyžaduje, aby všechny příkazy MFT , které se připojují ke správci front, poskytovaly pověření pro ID uživatele a heslo. Podobně může být při připojování k databázi vyžadováno, aby moduly protokolování MFT určily ID uživatele a heslo. Tyto informace o pověření lze uložit do souboru pověření MFT .

Informace o této úloze

Prvky v souboru `MQMFTCredentials.xml` musí odpovídat schématu `MQMFTCredentials.xsd` . Chcete-li získat informace o formátu `MQMFTCredentials.xml`, prohlédněte si Formát souboru pověření MFT.

Ukázkový soubor pověření najdete v adresáři `MQ_INSTALLATION_PATH/mqft/samples/credentials` .

Můžete mít jeden soubor pověření MFT pro koordinačního správce front, jeden pro správce front příkazů, jeden pro každého agenta a jeden pro každý modul protokolování. Alternativně můžete mít jeden soubor, který používá vše ve vaší topologii.

Výchozí umístění souboru pověření MFT je následující:

Linux AIX **AIX and Linux**

$HOME

Windows **Windows**

%USERPROFILE% nebo %HOMEDRIVE%%HOMEPATH%

Pokud je soubor pověření uložen v jiném umístění, můžete pomocí následujících vlastností určit, kde by jej měly příkazy hledat:

Tabulka 98. : Vlastnosti, které definují umístění souboru MQMFTCredentials.xml pro různé příkazy.

Typ příkazu	soubor vlastností	Název vlastnosti
Příkaz, který se připojuje ke koordinačnímu správci front	coordination.properties	coordinationQMgrAuthenticationCredentials
Příkaz, který se připojuje ke správci front příkazů	connection.properties	connectionQMgrAuthenticationCredentials
Příkaz, který se připojuje k procesu agenta	agent.properties	agentQMgrAuthenticationCredentials
Příkaz, který se připojuje k procesu modulu protokolování	logger.properties	loggerQMgrAuthenticationCredentials

Tabulka 99. : Vlastnosti, které definují umístění souboru MQMFTCredentials.xml pro agenty a procesy modulu protokolování.

Typ příkazu	soubor vlastností	Název vlastnosti
Agenti produktu MFT	agent.properties	agentQMgrAuthenticationCredentials
MFT Moduly protokolování	logger.properties	loggerQMgrAuthenticationCredentials

Podrobné informace o tom, které příkazy a procesy se připojují ke kterému správci front, naleznete v tématu Které MFT příkazy a procesy se připojují ke kterému správci front.

Namísto přidávání vlastností do jednotlivých souborů vlastností můžete přidat vlastnost **commonCredentialsKeyFile** do existujícího společného souboru `installation.properties` , aby agent, modul protokolování a příkazy mohly používat stejnou vlastnost.

Protože soubor pověření obsahuje informace o ID uživatele a hesle, vyžaduje speciální oprávnění, aby se zabránilo neoprávněnému přístupu k němu:

Linux AIX **AIX and Linux**

```
chown <agent owner userid>
chmod 600
```

Windows **Windows**

Ujistěte se, že dědičnost není povolena, a pak odeberte všechna ID uživatelů kromě těch, na kterých běží agent nebo modul protokolování, který bude používat soubor pověření.

Podrobnosti pověření použité pro připojení ke koordinačnímu správci front MFT v modulu plug-in IBM MQ Explorer Managed File Transfer závisí na typu konfigurace:

Globální (konfigurace na lokálním disku)

Globální konfigurace používá soubor pověření uvedený ve vlastnostech koordinace a příkazu.

Lokální (definováno v rámci IBM MQ Explorer):

Lokální konfigurace používá vlastnosti podrobností připojení přidruženého správce front v souboru IBM MQ Explorer.

Související úlohy

“Povolení ověření připojení pro produkt MFT” na stránce 597
Ověření připojení modulu plug-in IBM MQ Explorer MFT , který se připojuje ke koordinačnímu správci front nebo správci front příkazů, a ověření připojení pro agenta Managed File Transfer , který se připojuje ke koordinačnímu správci front nebo správci front příkazů, lze spustit v režimu kompatibility nebo v režimu ověření MQCSP.

Vytvoření struktury přenosu souborů IBM MQ

Související odkazy

Formát souboru pověření MFT

Šifrování uložených pověření v adresáři MFT

fteObfuscate: šifrovat citlivá data

z/OS Konfigurace `MQMFTCredentials.xml` na systému z/OS

Pokud je produkt Managed File Transfer (MFT) konfigurován s povoleným zabezpečením, ověření připojení vyžaduje všechny agenty MFT a příkazy, které se připojují ke správci front, aby bylo možné zadat pověření pro ID uživatele a heslo.

Podobně může být při připojování k databázi vyžadováno, aby moduly protokolování MFT určily ID uživatele a heslo.

Tyto informace o pověření lze uložit do souboru pověření MFT . Všimněte si, že soubory pověření jsou volitelné, je však snazší definovat soubor nebo soubory, které požadujete, než upravíte prostředí.

Kromě toho, pokud máte soubory pověření, obdržíte méně varovných zpráv. Varovné zprávy vás informují, že produkt MFT považuje zabezpečení správce front za vypnuté, a proto nezadáváte podrobnosti ověřování.

Ukázkový soubor pověření najdete v adresáři `MQ_INSTALLATION_PATH/mqft/samples/credentials` .

Zde je příklad souboru `MQMFTCredentials.xml`:

```
<?xml version="1.0" encoding="IBM-1047"?>
<tns:mqmftCredentials xmlns:tns="http://wmqfte.ibm.com/MFTCredentials"
xmlns:xsi="https://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://wmqfte.ibm.com/MFTCredentials MFTCredentials.xsd">
  <tns:qmgr name="MQPH" user="ADMIN" mqUserId="JOHNDOEH" mqPassword="cXXXX" />
  <tns:qmgr name="MQPI" user="ADMIN" mqUserId="JOHNDOEI" mqPassword="yXXXX" />
  <tns:qmgr name="MQPH" mqUserId="NONEH" mqPassword="yXXXX" />
  <tns:qmgr name="MQPI" mqUserId="NONEI" mqPassword="yXXXX" />
</tns:mqmftCredentials>
```

Když se úloha s ID uživatele ADMIN potřebuje připojit ke správci front MQPH, předá ID uživatele *JOHNDOEH* a použije heslo *cXXXX*.

Pokud je úloha spuštěna jiným ID uživatele a připojí MQPH, předá tato úloha ID uživatele *NONEH* a heslo *yXXXX*.

Výchozí umístění souboru `MQMFTCredentials.xml` je domovský adresář uživatele v systému z/OS UNIX System Services (USS). Je také možné uložit soubor buď do jiného umístění na USS, nebo do členu v rozdělené datové sadě.

Pokud je soubor pověření uložen v jiném umístění, můžete pomocí následujících vlastností určit, kde by jej měly příkazy hledat:

Tabulka 100. : Vlastnosti, které definují umístění souboru MQMFTCredentials.xml pro různé příkazy.

Typ příkazu	**soubor vlastností**	**Název vlastnosti**
Příkaz, který se připojuje ke koordinačnímu správci front	coordination.properties	coordinationQMgrAuthenticationCredentials
Příkaz, který se připojuje ke správci front příkazů	connection.properties	connectionQMgrAuthenticationCredentials
Příkaz, který se připojuje k procesu agenta	agent.properties	agentQMgrAuthenticationCredentials
Příkaz, který se připojuje k procesu modulu protokolování	logger.properties	loggerQMgrAuthenticationCredentials

Tabulka 101. : Vlastnosti, které definují umístění souboru MQMFTCredentials.xml pro agenty a procesy modulu protokolování.

Typ příkazu	**soubor vlastností**	**Název vlastnosti**
Agenti produktu MFT	agent.properties	agentQMgrAuthenticationCredentials
MFT Moduly protokolování	logger.properties	loggerQMgrAuthenticationCredentials

Podrobné informace o tom, které příkazy a procesy se připojují ke kterému správci front, naleznete v tématu Které MFT příkazy a procesy se připojují ke kterému správci front.

Chcete-li vytvořit soubor pověření v rámci rozdělené datové sady, postupujte takto:

- Vytvořte PDSE s formátem VB a délkou logického záznamu (Lrecl) 200.
- Vytvořte člen v rámci datové sady, poznamenejte si datovou sadu a člen a přidejte do členu následující kód:

```
<?xml version="1.0" encoding="IBM-1047"?>
<tns:mqmftCredentials xmlns:tns="http://wmqfte.ibm.com/MQMFTCredentials"
xmlns:xsi="https://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://wmqfte.ibm.com/MFTCredentials MQMFTCredentials.xsd">
```

```
  <!—-credentials information goes here-->
</tns:mqmftCredentials>
```

Soubor pověření můžete chránit pomocí produktu zabezpečení, například RACF, ale ID uživatelů spouštějící příkazy Managed File Transfer a spravující procesy agenta a modulu protokolování vyžadují přístup pro čtení k tomuto souboru.

Informace v tomto souboru můžete zakrývat pomocí JCL ve členu BFGCROBS. Toto vezme soubor a zašifruje ID a heslo uživatele IBM MQ . Například člen BFGCROBS vezme řádek

```
<tns:qmgr name="MQPI" user="JOHNDOE2" mqUserId="JOHNDOE1" mqPassword="yXXXX" />
```

a vytváří

```
<tns:qmgr mqPasswordCipher="e977c61e9b9c363c" mqUserIdCipher="c394c5887867157c"
name="MQPI" user="JOHNDOE2"/>
```

Chcete-li zachovat mapování ID uživatele na ID uživatele IBM MQ , můžete do souboru přidat komentáře. Například:

```
<!--      name="MQPI" user="ADMIN"    mqUserId="JOHNDOE1 -->
```

Tyto připomínky jsou procesem zamlžení nezměněny.

Všimněte si, že obsah je skrytý, není silně šifrovaný. Měli byste omezit, která ID uživatelů mají přístup k souboru.

Související úlohy

“Konfigurace souboru MQMFTCredentials.xml na platformě Multiplatforms” na stránce 594
Je-li Managed File Transfer (MFT) nakonfigurován s povoleným zabezpečením, ověření připojení vyžaduje, aby všechny příkazy MFT , které se připojují ke správci front, poskytovaly pověření pro ID uživatele a heslo. Podobně může být při připojování k databázi vyžadováno, aby moduly protokolování MFT určily ID uživatele a heslo. Tyto informace o pověření lze uložit do souboru pověření MFT .

Povolení ověření připojení pro produkt MFT

Ověření připojení modulu plug-in IBM MQ Explorer MFT , který se připojuje ke koordinačnímu správci front nebo správci front příkazů, a ověření připojení pro agenta Managed File Transfer , který se připojuje ke koordinačnímu správci front nebo správci front příkazů, lze spustit v režimu kompatibility nebo v režimu ověření MQCSP.

Informace o této úloze

Před verzí IBM MQ 9.2.0je výchozím nastavením pro ověřování připojení režim kompatibility. Můžete však zakázat výchozí režim kompatibility a povolit režim ověřování MQCSP.

V produktu IBM MQ 9.2.0je výchozí režim ověřování MQCSP.

Pro ověření připojení pro modul plug-in IBM MQ Explorer Managed File Transfer nebo pro agenty Managed File Transfer , kteří se připojují ke správci front pomocí přenosu CLIENT, jsou hesla delší než 12 znaků podporována pouze pro režim ověření MQCSP. Pokud při autorizaci pomocí režimu kompatibility zadáte heslo delší než 12 znaků, dojde k chybě a agent se neověří u správce front. Viz zpráva BFGAG0187E v části Diagnostické zprávy: BFGAG0001 - BFGAG9999.

Procedura

- Chcete-li vybrat režim ověřování připojení pro koordinačního správce front nebo správce front příkazů v produktu IBM MQ Explorer, postupujte takto:
  a) Vyberte správce front, ke kterému se chcete připojit.
  b) Klepněte pravým tlačítkem myši a z rozevírací nabídky vyberte volbu **Podrobnosti připojení-> Vlastnosti** .

c) Klepněte na kartu **ID uživatele**.

d) Ujistěte se, že je zaškrtnuto políčko pro režim ověřování připojení, který chcete použít:

- V systému IBM MQ 9.1.0není standardně zaškrtnuto políčko **Režim kompatibility identifikace uživatele** . To znamená, že pokud je zaškrtnuto políčko **Povolit identifikaci uživatele** , bude produkt IBM MQ Explorer při připojování ke správci front používat ověřování MQCSP. Pokud se produkt IBM MQ Explorer potřebuje připojit ke správci front pomocí režimu kompatibility namísto ověřování MQCSP, zkontrolujte, zda jsou zaškrtnuta políčka **Povolit identifikaci uživatele** a **Režim kompatibility identifikace uživatele** .
- Před IBM MQ 9.1.0je standardně označeno zaškrtávací políčko **Režim kompatibility identifikace uživatele** . To znamená, že pokud je zaškrtnuto políčko **Povolit identifikaci uživatele** , bude produkt IBM MQ Explorer při připojování ke správci front používat režim kompatibility. Pokud se produkt IBM MQ Explorer potřebuje připojit ke správci front pomocí ověřování MQCSP, zkontrolujte, zda je zaškrtnuto políčko **Povolit identifikaci uživatele** a zda není zaškrtnuto políčko **Režim kompatibility identifikace uživatele** .

- Chcete-li povolit nebo zakázat režim ověření MQCSP pro agenta Managed File Transfer pomocí souboru `MQMFTCredentials.xml` , přidejte parametr **`useMQCSPAuthentication`** do souboru `MQMFTCredentials.xml` pro příslušného uživatele.

  Parametr **`useMQCSPAuthentication`** má následující hodnoty:

  ano
  Režim ověřování MQCSP se používá k ověření uživatele se správcem front.

  V poli IBM MQ 9.2.0je výchozí hodnotou hodnota `true` . Není-li parametr **`useMQCSPAuthentication`** určen, je standardně nastaven na hodnotu `true` a k ověření uživatele se správcem front je použit režim ověřování MQCSP.

  ne
  Režim kompatibility se používá k ověření uživatele se správcem front.

  Není-li parametr **`useMQCSPAuthentication`** zadán, je před parametrem IBM MQ 9.2.0standardně nastaven na hodnotu `false` a k ověření uživatele u správce front je použit režim kompatibility.

  Následující příklad uvádí, jak nastavit parametr **`useMQCSPAuthentication`** v souboru `MQMFTCredentials.xml` :

```
<tns:qmgr name="CoordQueueMgr" user="ernest" mqUserId="ernest"
    mqPassword="AveryL0ngPassw0rd2135" useMQCSPAuthentication="true"/>
```

Související pojmy

“Ochrana heslem MQCSP” na stránce 31
Ověřovací pověření uvedená ve struktuře MQCSP mohou být buď chráněna pomocí funkce ochrany heslem produktu IBM MQ MQCSP, nebo šifrována pomocí šifrování TLS.

Související odkazy

“Ověření připojení MFT a IBM MQ” na stránce 593
Ověřování připojení umožňuje konfigurovat správce front pro ověřování aplikací pomocí zadaného jména uživatele a hesla. Pokud má přidružený správce front povoleno zabezpečení a vyžaduje podrobnosti o pověření (ID uživatele a heslo), musí být před úspěšným připojením ke správci front povolena funkce ověřování připojení. Ověřování připojení lze spustit v režimu kompatibility nebo v režimu ověřování MQCSP.

Formát souboru pověření MFT

MFT pískoviště

Můžete omezit oblast systému souborů, ke které má agent přístup v rámci přenosu. Oblast, pro kterou je agent omezen, se nazývá sandbox. Můžete použít omezení buď na agenta, nebo na uživatele, který požaduje přenos.

Pískoviště nejsou podporována, pokud je agent agentem mostu protokolů nebo agentem mostu Connect:Direct . Nemůžete použít pískoviště agenta pro agenty, kteří potřebují přenést do nebo z front IBM MQ .

Související odkazy

“Práce s pískovišti agenta MFT” na stránce 599
Chcete-li přidat další úroveň zabezpečení do produktu Managed File Transfer, můžete omezit oblast systému souborů, ke které má agent přístup.

“Práce s pískovišti uživatele MFT” na stránce 600
Můžete omezit oblast systému souborů, do které mohou být soubory přenášeny a ze které mohou být odvozeny, na základě jména uživatele MQMD, který požaduje přenos.

Práce s pískovišti agenta MFT

Chcete-li přidat další úroveň zabezpečení do produktu Managed File Transfer, můžete omezit oblast systému souborů, ke které má agent přístup.

Pro agenty, kteří se přenášejí do front IBM MQ nebo z nich, nelze použít pískoviště agenta. Omezení přístupu k frontám IBM MQ s pískovištním boxem lze implementovat namísto použití pískoviště uživatele, což je doporučené řešení pro všechny požadavky na pískování. Další informace o pískování uživatelů viz “Práce s pískovišti uživatele MFT” na stránce 600

Chcete-li povolit pískoviště agenta, přidejte následující vlastnost do souboru `agent.properties` pro agenta, kterého chcete omezit:

```
sandboxRoot=[!]restricted_directory_nameseparator...separator[!]restricted_directory_name
```

kde:

- *`restricted_directory_name`* je cesta k adresáři, která má být povolena nebo odepřena.
- Parametr `!` je volitelný a určuje, že následující hodnota parametru *`restricted_directory_name`* je odepřena (vyloučena). Pokud `!` není uvedeno *`restricted_directory_name`* , je povolená (zahrnutá) cesta.
- *`separator`* je oddělovač specifický pro platformu.

Chcete-li například omezit přístup, který má AGENT1 , pouze k adresáři `/tmp` , ale nepovolit přístup k podadresáři `private` , nastavte vlastnost v souboru `agent.properties` , který patří k AGENT1: `sandboxRoot=/tmp:!/tmp/private`.

Vlastnost sandboxRoot je popsána v části Rozšířené vlastnosti agenta.

Agent i uživatelské pískoviště nejsou podporovány v agentech mostu protokolů ani v agentech mostu Connect:Direct .

Práce v sandboxu na platformách AIX, Linux, and Windows

ALW Na platformách AIX, Linux, and Windows pískoviště omezuje, ze kterých adresářů může agent Managed File Transfer Agent číst a do kterých může zapisovat. Při aktivaci sandboxu může agent Managed File Transfer Agent číst a zapisovat do adresářů určených jako povolené a do všech podadresářů, které uvedené adresáře obsahují, pokud nejsou v adresáři sandboxRooturčeny jako odepřené podadresáře. Pískoviště Managed File Transfer nemá přednost před zabezpečením operačního systému. Uživatel, který spustil produkt Managed File Transfer Agent , musí mít odpovídající přístup na úrovni operačního systému k libovolnému adresáři, aby mohl číst z adresáře nebo do něj zapisovat. Symbolický odkaz na adresář není následován, pokud je odkazovaný adresář mimo určené adresáře sandboxRoot (a podadresáře).

Práce v sandboxu na z/OS

z/OS V systému z/OSpískoviště omezuje kvalifikátory názvů datových sad, ze kterých může produkt Managed File Transfer Agent číst a do kterých může zapisovat. Uživatel, který spustil produkt Managed File Transfer Agent , musí mít správná oprávnění operačního systému pro všechny zahrnuté datové sady. Pokud uzavřete hodnotu kvalifikátoru názvu datové sady sandboxRoot do dvojitých uvozovek, hodnota se řídí běžnou konvencí z/OS a je považována za plně kvalifikovanou. Vynecháte-li dvojité uvozovky, bude před sandboxRoot uvedeno aktuální ID uživatele. Pokud například nastavíte vlastnost sandboxRoot na následující: `sandboxRoot=//test`, agent bude mít přístup k následujícím datovým sadám (ve standardní z/OS notaci) *//username*`.test.**` Za běhu, pokud počáteční úrovně plně vyřešeného názvu datové sady neodpovídají sandboxRoot, požadavek na přenos bude odmítnut.

Práce v sandboxu na systémech IBM i

IBM i V případě souborů v integrovaném systému souborů na systémech IBM i pískoviště omezuje, ze kterých adresářů může produkt Managed File Transfer Agent číst a do kterých může zapisovat. Při aktivaci sandboxu může agent Managed File Transfer Agent číst a zapisovat do adresářů určených jako povolené a do všech podadresářů, které uvedené adresáře obsahují, pokud nejsou v adresáři sandboxRooturčeny jako odepřené podadresáře. Pískoviště Managed File Transfer nemá přednost před zabezpečením operačního systému. Uživatel, který spustil produkt Managed File Transfer Agent , musí mít odpovídající přístup na úrovni operačního systému k libovolnému adresáři, aby mohl číst z adresáře nebo do něj zapisovat. Symbolický odkaz na adresář není následován, pokud je odkazovaný adresář mimo určené adresáře sandboxRoot (a podadresáře).

Související odkazy

“Další kontroly pro přenosy se zástupnými znaky” na stránce 603
Pokud byl agent nakonfigurován s uživatelem nebo se sandboxem agenta, aby se omezila umístění, ze kterých může agent přenášet soubory, můžete určit, že se mají provádět další kontroly přenosů se zástupnými znaky pro tohoto agenta.

“Práce s pískovišti agenta MFT” na stránce 599
Chcete-li přidat další úroveň zabezpečení do produktu Managed File Transfer, můžete omezit oblast systému souborů, ke které má agent přístup.

Soubor MFT `agent.properties`

Práce s pískovišti uživatele MFT

Můžete omezit oblast systému souborů, do které mohou být soubory přenášeny a ze které mohou být odvozeny, na základě jména uživatele MQMD, který požaduje přenos.

Pískoviště uživatelů nejsou podporována, pokud je agent agentem mostu protokolů nebo agentem mostu Connect:Direct .

Chcete-li povolit pískoviště uživatele, přidejte následující vlastnost do souboru `agent.properties` pro agenta, kterého chcete omezit:

```
userSandboxes=true
```

Je-li tato vlastnost přítomna a nastavena na hodnotu true, agent použije informace v souboru *MQ_DATA_PATH*`/mqft/config/`*coordination_qmgr_name*`/agents/`*agent_name*`/UserSandboxes.xml` k určení, ke kterým částem systému souborů má uživatel, který požaduje přenos, přístup.

Soubor `UserSandboxes.xml` XML se skládá z prvku <agent> , který obsahuje nula nebo více prvků <sandbox> . Tyto prvky popisují, která pravidla se použijí na které uživatele. Atribut `user` prvku <sandbox> je vzor, který se používá k porovnání s uživatelem MQMD požadavku.

Agent pravidelně znovu načítá soubor `UserSandboxes.xml` a všechny platné změny souboru ovlivní chování agenta. Výchozí interval opětovného načtení je 30 sekund. Tento interval lze změnit určením vlastnosti agenta xmlConfigReloadInterval v souboru `agent.properties` .

Zadáte-li atribut nebo hodnotu `userPattern="regex"` , bude atribut `user` interpretován jako regulární výraz Java . Další informace viz Regulární výrazy používané MFT.

Pokud neuvedete atribut `userPattern="regex"` nebo hodnotu, bude atribut `user` interpretován jako vzor s následujícími zástupnými znaky:

- hvězdička (*), která představuje nula nebo více znaků
- otazník (?), který představuje právě jeden znak

Shody se provádějí v pořadí, v jakém jsou prvky `<sandbox>` uvedeny v souboru. Použije se pouze první shoda, všechny následující potenciální shody v souboru jsou ignorovány. Pokud se žádný z prvků `<sandbox>` uvedených v souboru neshoduje s uživatelem MQMD přidruženým ke zprávě požadavku na přenos, přenos nemůže přistupovat k systému souborů. Pokud byla nalezena shoda mezi jménem uživatele MQMD a atributem `user` , tato shoda identifikuje sadu pravidel uvnitř prvku `<sandbox>` , která jsou použita na přenos. Tato sada pravidel se používá k určení, které souborynebo datové sady lze načíst nebo zapsat jako součást přenosu.

Každá sada pravidel může určovat prvek `<read>` , který identifikuje, které soubory lze číst, a prvek `<write>` , který identifikuje, které soubory lze zapsat. Vynecháte-li prvky `<read>` nebo `<write>` ze sady pravidel, předpokládá se, že uživatel přidružený k této sadě pravidel nebude moci podle potřeby provádět žádná čtení ani zápis.

Poznámka: Prvek `<read>` musí být před prvkem `<write>` a prvek `<include>` musí být před prvkem `<exclude>` v souboru `UserSandboxes.xml` .

Každý prvek `<read>` nebo `<write>` obsahuje jeden nebo více vzorů, které se používají k určení, zda je soubor v sandboxu a lze jej přenést. Tyto vzory zadejte pomocí prvků `<include>` a `<exclude>` . Atribut `name` prvku `<include>` nebo `<exclude>` uvádí vzor, který se má porovnat. Volitelný atribut `type` uvádí, zda je hodnota názvu souborem nebo vzorem fronty. Pokud není uveden atribut `type` , agent bude se vzorem zacházet jako se vzorem cesty k souboru nebo adresáři. Příklad:

```
<tns:read>
    <tns:include name="/home/user/**"/>
    <tns:include name="USER.**" type="queue"/>
    <tns:exclude name="/home/user/private/**"/>
</tns:read>
```

Vzory `<include>` a `<exclude>` `name` používá agent k určení, zda lze soubory, datové sady nebo fronty číst nebo do nich zapisovat. Operace je povolena, pokud kanonická cesta k souboru, datová sada nebo název fronty odpovídá alespoň jednomu ze zahrnutých vzorů a přesně nule vyloučených vzorů. Vzory určené pomocí atributu `name` prvků `<include>` a `<exclude>` používají oddělovače cest a konvence odpovídající platformě, na které je agent spuštěn. Zadáte-li relativní cesty k souborům, budou tyto cesty interpretovány relativně vzhledem k vlastnosti `transferRoot` agenta.

Při zadávání omezení fronty je podporována syntaxe QUEUE@QUEUEMANAGER s následujícími pravidly:

- Pokud v položce chybí znak zavináč (@), je vzor považován za název fronty, ke kterému lze přistupovat v libovolném správci front. Pokud je například vzor `name` , zachází se s ním stejným způsobem jako s `name@**`.
- Je-li znak zavináč (@) prvním znakem v položce, je vzor považován za název správce front a lze přistupovat ke všem frontám ve správci front. Pokud je například vzor `@name` , bude se s ním zacházet stejně jako s `**@name`.

Následující zástupné znaky mají speciální význam, když je zadáte jako součást atributu `name` prvků `<include>` a `<exclude>` :

*****

Jedna hvězdička se shoduje s žádným nebo více znaky v názvu adresáře nebo v kvalifikátoru názvu datové sady nebo názvu fronty.

?

Otazník odpovídá přesně jednomu znaku v názvu adresáře nebo kvalifikátoru názvu datové sady nebo názvu fronty.

**
Dva znaky hvězdičky se neshodují s žádným nebo více názvy adresářů nebo s žádným či více kvalifikátory v názvu datové sady nebo názvu fronty. Také cesty, které končí oddělovačem cest, mají na konec cesty přidáno implicitní "**" . Takže /home/user/ je stejné jako /home/user/**.

Příklad:

- /**/test/** odpovídá libovolnému souboru, který má v cestě adresář test
- /test/file? odpovídá libovolnému souboru v adresáři /test , který začíná řetězcem file následovaným libovolným jedním znakem
- c:\test*.txt odpovídá libovolnému souboru v adresáři c:\test s příponou .txt
- c:\test***.txt odpovídá libovolnému souboru v adresáři 'c:\test nebo v jednom z jeho podadresářů s příponou .txt .
- z/OS //'TEST.*.DATA' odpovídá libovolné datové sadě, která má první kvalifikátor TEST, má jakýkoli druhý kvalifikátor a třetí kvalifikátor DATA.
- *@QM1 odpovídá libovolné frontě ve správci front QM1 , která má jeden kvalifikátor.
- TEST.*.QUEUE@QM1 odpovídá libovolné frontě ve správci front QM1 , která má první kvalifikátor TEST, má jakýkoli druhý kvalifikátor a třetí kvalifikátor QUEUE.
- **@QM1 odpovídá libovolné frontě ve správci front QM1.

Symbolické odkazy

Všechny symbolické odkazy, které používáte v cestách k souborům v souboru UserSandboxes.xml , musíte plně vyřešit zadáním pevných odkazů v prvcích <include> a <exclude> . Máte-li například symbolický odkaz, kde /var mapuje na /SYSTEM/var, musíte tuto cestu zadat jako <tns:include name="/SYSTEM/var"/>, jinak se zamýšlený přenos nezdaří s chybou zabezpečení pískoviště uživatele.

Příklad

Tento příklad ukazuje, jak povolit uživateli se jménem uživatele MQMD guest přenos libovolného souboru z adresáře /home/user/public nebo libovolného jeho podadresáře na systému, kde je spuštěn agent AGENT_JUPITER, přidáním následujícího prvku <sandbox> do souboru UserSandboxes.xml v konfiguračním adresáři AGENT_JUPITER:

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:userSandboxes
        xmlns:tns="http://wmqfte.ibm.com/UserSandboxes"
        xmlns:xsi="https://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="http://wmqfte.ibm.com/UserSandboxes UserSandboxes.xsd">
    <tns:agent>
        <tns:sandbox user="guest">
            <tns:read>
                <tns:include name="/home/user/public/**"/>
             </tns:read>
        </tns:sandbox>
    </tns:agent>
</tns:userSandboxes>
```

Příklad

Tento příklad ukazuje, jak umožnit libovolnému uživateli se jménem uživatele MQMD account následovaným jednou číslicí, například account4, provést následující akce:

- Přeneste libovolný soubor z adresáře /home/account nebo z jeho podadresářů, s výjimkou adresáře /home/account/private na systému, kde je spuštěn agent AGENT_SATURN.
- Přeneste libovolný soubor do adresáře /home/account/output nebo do libovolného jeho podadresáře na systému, kde je spuštěn agent AGENT_SATURN.

- Číst zprávy z front v lokálním správci front počínaje předponou `ACCOUNT.` , pokud nezačíná předponou `ACCOUNT.PRIVATE.` (tj. `PRIVATE` na druhé úrovni).
- Přeneste data do front začínajících předponou `ACCOUNT.OUTPUT.` v libovolném správci front.

Chcete-li povolit uživateli se jménem uživatele MQMD `account` dokončit tyto akce, přidejte do souboru `UserSandboxes.xml`v konfiguračním adresáři AGENT_SATURN následující prvek `<sandbox>` :

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:userSandboxes
            xmlns:tns="http://wmqfte.ibm.com/UserSandboxes"
            xmlns:xsi="https://www.w3.org/2001/XMLSchema-instance"
            xsi:schemaLocation="http://wmqfte.ibm.com/UserSandboxes UserSandboxes.xsd">
    <tns:agent>
        <tns:sandbox user="account[0-9]" userPattern="regex">
            <tns:read>
                <tns:include name="/home/account/**"/>
                <tns:include name="ACCOUNT.**" type="queue"/>
                <tns:exclude name="ACCOUNT.PRIVATE.**" type="queue"/>
                <tns:exclude name="/home/account/private/**"/>
                                                    </tns:read>
            <tns:write>
                <tns:include name="/home/account/output/**"/>
                <tns:include name="ACCOUNT.OUTPUT.**" type="queue"/>
            </tns:write>
        </tns:sandbox>
    </tns:agent>
</tns:userSandboxes>
```

Související odkazy

“Další kontroly pro přenosy se zástupnými znaky” na stránce 603
Pokud byl agent nakonfigurován s uživatelem nebo se sandboxem agenta, aby se omezila umístění, ze kterých může agent přenášet soubory, můžete určit, že se mají provádět další kontroly přenosů se zástupnými znaky pro tohoto agenta.

Soubor MFT `agent.properties`

Další kontroly pro přenosy se zástupnými znaky

Pokud byl agent nakonfigurován s uživatelem nebo se sandboxem agenta, aby se omezila umístění, ze kterých může agent přenášet soubory, můžete určit, že se mají provádět další kontroly přenosů se zástupnými znaky pro tohoto agenta.

Vlastnost additionalWildcardSandboxChecking

Chcete-li povolit další kontrolu přenosů se zástupnými znaky, přidejte následující vlastnost do souboru `agent.properties` pro agenta, kterého chcete zkontrolovat.

```
additionalWildcardSandboxChecking=true
```

Je-li tato vlastnost nastavena na hodnotu true a agent provede požadavek na přenos, který se pokusí načíst umístění mimo definovaný sandbox pro porovnávání souborů se zástupným znakem, přenos se nezdaří. Pokud v rámci jednoho požadavku na přenos existuje více přenosů a jeden z těchto požadavků se nezdaří kvůli pokusu o čtení umístění mimo pískoviště, celý přenos se nezdaří. Pokud kontrola selže, příčina selhání je uvedena v chybové zprávě.

Pokud je vlastnost additionalWildcardSandboxChecking vynechána ze souboru `agent.properties` agenta nebo je nastavena na hodnotu false, nebudou provedeny žádné další kontroly přenosů se zástupnými znaky pro tohoto agenta.

Chybové zprávy pro kontrolu zástupných znaků

Níže jsou uvedeny zprávy, které jsou hlášeny při zadání požadavku na přenos se zástupnými znaky do umístění mimo nakonfigurované umístění sandboxu.

Následující zpráva se vyskytne, když je cesta k souboru se zástupným znakem v požadavku na přenos umístěna mimo omezený sandbox:

```
BFGSS0077E: Pokus o čtení cesty k souboru: path byl odepřen.
Cesta k souboru je umístěna mimo omezené přenosové prostředí sandbox.
```

Následující zpráva se vyskytne, když přenos v rámci požadavku na přenos s více zástupnými znaky obsahuje požadavek na přenos, kde je cesta umístěna mimo omezené pískoviště:

```
BFGSS0078E: Pokus o čtení cesty k souboru: path byl ignorován jako jiný přenos.
Položka ve spravovaném přenosu se pokusila číst mimo omezené přenosové pískoviště.
```

Pokud je soubor umístěn mimo omezený sandbox, zobrazí se následující zpráva:

```
BFGSS0079E: Pokus o čtení souboru cesta k souboru byl odepřen.
Soubor je umístěn mimo omezené přenosové prostředí sandbox.
```

Následující zpráva se vyskytuje ve vícenásobném požadavku na přenos, kde jiný požadavek na přenos se zástupnými znaky způsobil ignorování tohoto požadavku:

```
BFGSS0080E: Pokus o čtení souboru: cesta k souboru byl ignorován jako jiný přenos.
Položka ve spravovaném přenosu se pokusila číst mimo omezené přenosové pískoviště.
```

V případě přenosů jednotlivých souborů, které nezahrnují zástupné znaky, se zpráva, která je ohlášena, když přenos zahrnuje soubor umístěný mimo sandbox, od předchozích verzí nezměnila:

```
Selhání s BFGIO0056E: Pokus o čtení souboru "FILE" byl odepřen.
Soubor je umístěn mimo omezené přenosové prostředí sandbox.
```

Související odkazy

“Práce s pískovišti uživatele MFT” na stránce 600
Můžete omezit oblast systému souborů, do které mohou být soubory přenášeny a ze které mohou být odvozeny, na základě jména uživatele MQMD, který požaduje přenos.

“Práce s pískovišti agenta MFT” na stránce 599
Chcete-li přidat další úroveň zabezpečení do produktu Managed File Transfer, můžete omezit oblast systému souborů, ke které má agent přístup.

Soubor MFT `agent.properties`

Konfigurace šifrování SSL nebo TLS pro MFT

Zabezpečení SSL nebo TLS lze použít spolu s produktem IBM MQ Managed File Transfer k zabezpečení komunikace mezi agenty a jejich správci front agenta, příkazy a správci front, ke kterým se připojují, a různými správci front pro připojení správců front v rámci topologie.

Než začnete

K šifrování zpráv, které procházejí topologií produktu IBM MQ Managed File Transfer , můžete použít šifrování SSL nebo TLS. Patří k nim:

- Zprávy předávané mezi agentem a jeho správcem front agenta.
- Zprávy pro příkazy a správce front, ke kterým se připojují.
- Interní zprávy, které se pohybují mezi správci front agenta, správci front příkazů a koordinačním správcem front v rámci topologie.

Informace o této úloze

Obecné informace o použití SSL s produktem IBM MQnaleznete v části “Práce s SSL/TLS” na stránce 276. V termínech IBM MQ je Managed File Transfer standardní klientská aplikace Java .

Chcete-li použít zabezpečení SSL s produktem Managed File Transfer, postupujte takto:

Postup

1. Vytvořte soubor úložiště údajů o důvěryhodnosti a volitelně i soubor úložiště klíčů (tyto soubory mohou být stejné). Pokud nepotřebujete ověření klienta (tj. v kanálech SSLCAUTH=OPTIONAL), nemusíte

poskytovat úložiště klíčů. K ověření certifikátu správce front je vyžadováno pouze úložiště údajů o důvěryhodnosti.

Algoritmus klíče použitý pro vytvoření certifikátů pro úložiště údajů o důvěryhodnosti a úložiště klíčů musí být RSA pro práci s produktem IBM MQ.

2. Nastavte správce front IBM MQ tak, aby používal zabezpečení SSL.

   Informace o nastavení správce front pro použití zabezpečení SSL pomocí produktu IBM MQ Explorer naleznete například v tématu Konfigurace zabezpečení SSL ve správcích front.
3. Uložte soubor úložiště údajů o důvěryhodnosti a soubor úložiště klíčů (pokud jej máte) do vhodného umístění. Navrhovaným umístěním je adresář *config_directory*/*coordination_qmgr*/agents/*agent_name* .
4. Nastavte vlastnosti zabezpečení SSL podle potřeby pro každého správce front s povoleným zabezpečením SSL v příslušném souboru vlastností Managed File Transfer . Každá sada vlastností odkazuje na samostatného správce front (agenta, koordinaci a příkaz), ačkoli jeden správce front může provádět dvě nebo více těchto rolí.

   Je vyžadována jedna z vlastností **CipherSpec** nebo **CipherSuite** , jinak se klient pokusí připojit bez zabezpečení SSL. Obě vlastnosti **CipherSpec** nebo **CipherSuite** jsou poskytnuty kvůli terminologickým rozdílům mezi IBM MQ a Java. Produkt Managed File Transfer přijímá obě vlastnosti a provádí nezbytný převod, takže nemusíte nastavovat obě vlastnosti. Pokud zadáte obě vlastnosti **CipherSpec** nebo **CipherSuite** , bude mít přednost **CipherSpec** .

   Vlastnost **PeerName** je volitelná. Vlastnost můžete nastavit na rozlišující název správce front, ke kterému se chcete připojit. Produkt Managed File Transfer odmítne připojení k chybnému serveru SSL s rozlišujícím názvem, který se neshoduje.

   Nastavte vlastnosti **SslTrustStore** a **SslKeyStore** na názvy souborů, které ukazují na úložiště údajů o důvěryhodnosti a soubory úložiště klíčů. Pokud nastavujete tyto vlastnosti pro agenta, který je již spuštěn, zastavte a restartujte agenta, abyste se znovu připojili v režimu SSL.

   Soubory vlastností obsahují hesla ve formátu prostého textu, proto zvažte nastavení příslušných oprávnění systému souborů.

   Další informace o vlastnostech SSL viz “Vlastnosti SSL/TLS pro MFT” na stránce 605.
5. Pokud správce front agenta používá zabezpečení SSL, nemůžete při vytváření agenta poskytnout nezbytné podrobnosti. Chcete-li vytvořit agenta, postupujte takto:
   a) Vytvořte agenta pomocí příkazu **fteCreateAgent** . Zobrazí se varování o tom, že nelze publikovat existenci agenta do koordinačního správce front.
   b) Upravte soubor `agent.properties` , který byl vytvořen v předchozím kroku, abyste přidali informace o SSL. Po úspěšném spuštění agenta se znovu provede pokus o publikování.
6. Pokud jsou agenti nebo instance průzkumníku IBM MQ spuštěni při změně vlastností SSL v souboru `agent.properties` nebo `coordination.properties` , musíte restartovat agenta nebo IBM MQ Explorer.

Související odkazy

Soubor MFT `agent.properties`

Vlastnosti SSL/TLS pro MFT

Některé soubory vlastností MFT zahrnují vlastnosti SSL a TLS. Můžete použít zabezpečení SSL nebo TLS s protokoly IBM MQ a Managed File Transfer , chcete-li zabránit neoprávněnému připojení mezi agenty a správci front a šifrovat provoz zpráv mezi agenty a správci front.

Následující soubory vlastností MFT zahrnují vlastnosti SSL:

- Vlastnosti SSL/TLS pro soubor MFT `agent.properties`
- Vlastnosti SSL/TLS pro soubor MFT `coordination.properties`
- Vlastnosti SSL/TLS pro soubor MFT `command.properties`
- Vlastnosti SSL/TLS pro soubor MFT `logger.properties`

Chcete-li získat informace o použití SSL nebo TLS s produktem Managed File Transfer, prohlédněte si téma “Konfigurace šifrování SSL nebo TLS pro MFT” na stránce 604.

V produktu IBM WebSphere MQ 7.5můžete použít proměnné prostředí v některých vlastnostech Managed File Transfer , které představují umístění souborů nebo adresářů. To umožňuje, aby se umístění souborů nebo adresářů, které se používají při spouštění částí produktu, lišila v závislosti na změnách prostředí, například na tom, který uživatel spouští proces. Další informace viz Použití proměnných prostředí ve MFT vlastnostech.

Související pojmy

Volby konfigurace MFT na platformě Multiplatforms

Související odkazy

Použití proměnných prostředí ve vlastnostech MFT

Připojení ke správci front v režimu klienta s ověřením kanálu

Produkt IBM MQ používá záznamy ověřování kanálu k přesnějšímu řízení přístupu na úrovni kanálu. To znamená, že nově vytvoření správci front standardně odmítají připojení klienta z komponenty Managed File Transfer .

Další informace o ověřování kanálu viz “Záznamy ověření kanálu” na stránce 51.

Pokud konfigurace ověřování kanálu pro SVRCONN používaný produktem Managed File Transfer uvádí neprivilegované ID MCAUSER, musíte udělit specifické záznamy oprávnění pro správce front, fronty a témata, aby mohl produkt Managed File Transfer Agent a příkazy správně pracovat. Použijte příkaz MQSC SET CHLAUTH nebo příkaz PCF Set Channel Authentication Record k vytvoření, úpravě nebo odebrání záznamů ověření kanálu. Pro všechny agenty Managed File Transfer , které chcete připojit ke správci front IBM MQ , můžete buď nastavit ID MCAUSER pro všechny agenty, nebo pro každého agenta nastavit samostatné ID MCAUSER.

Udělte každému ID uživatele MCAUSER následující oprávnění:

- Záznamy oprávnění požadované pro správce front:
  - connect
  - setid
  - inq
- Záznamy oprávnění požadované pro fronty.

  Pro všechny fronty specifické pro agenta, tj. názvy front, které končí na *název_agenta* v následujícím seznamu, musíte vytvořit tyto záznamy oprávnění fronty pro každého agenta, kterého chcete připojit ke správci front IBM MQ pomocí připojení klienta.
  - put, get, dsp (SYSTEM.DEFAULT.MODEL.QUEUE)
  - vložit, získat, setid, procházet (SYSTEM.FTE.COMMAND.*název_agenta*)
  - put, get (SYSTEM.FTE.DATA.*název_agenta*)
  - put, get (SYSTEM.FTE.REPLY.*název_agenta*)
  - put, get, inq, browse (vložení, získání, inq, procházení) (SYSTEM.FTE.STATE.*název_agenta*)
  - put, get, browse (vložení, získání, procházení) (SYSTEM.FTE.EVENT.*název_agenta*)
  - put, get (SYSTEM.FTE)
- Záznamy oprávnění požadované pro témata:
  - sub, pub (SYSTEM.FTE)
- Záznamy oprávnění požadované pro přenosy souborů.

  Máte-li oddělená ID MCAUSER pro zdrojového a cílového agenta, vytvořte záznamy oprávnění ve frontách agentů ve zdroji i v místě určení.

  Pokud je například ID MCAUSER zdrojového agenta **user1** a ID MCAUSER cílového agenta je **user2**, nastavte pro uživatele agenta následující oprávnění:

Uživatel AGENT	Fronta	Požadované oprávnění
user1	SYSTEM.FTE.DATA.*název_cílového_agenta*	put
user1	SYSTEM.FTE.COMMAND.*název_cílového_agenta*	put
user2	SYSTEM.FTE.REPLY.*název_zdrojového_agenta*	put
user2	SYSTEM.FTE.COMMAND.*název_zdrojového_agenta*	put

Konfigurace zabezpečení SSL nebo TLS mezi agentem mostu Connect:Direct a uzlem Connect:Direct

Nakonfigurujte agenta mostu Connect:Direct a uzel Connect:Direct tak, aby se vzájemně připojovaly prostřednictvím protokolu SSL, a to vytvořením úložiště klíčů a úložiště údajů o důvěryhodnosti a nastavením vlastností v souboru vlastností agenta mostu Connect:Direct .

Informace o této úloze

Tyto kroky zahrnují pokyny pro získání klíčů podepsaných certifikační autoritou. Pokud nepoužíváte certifikační autoritu, můžete vygenerovat certifikát podepsaný svým držitelem. Další informace o generování certifikátu podepsaného (svým) držitelem viz “Práce se zabezpečením SSL/TLS v systému AIX, Linux, and Windows” na stránce 293.

Tyto kroky zahrnují pokyny pro vytvoření nového úložiště klíčů a úložiště údajů o důvěryhodnosti pro agenta mostu Connect:Direct . Pokud již agent mostu Connect:Direct má úložiště klíčů a úložiště údajů o důvěryhodnosti, které používá k bezpečnému připojení ke správcům front IBM MQ , můžete použít existující úložiště klíčů a úložiště údajů o důvěryhodnosti při bezpečném připojení k uzlu Connect:Direct . Další informace viz “Konfigurace šifrování SSL nebo TLS pro MFT” na stránce 604.

Postup

V případě uzlu Connect:Direct postupujte takto:

1. Vygenerujte klíč a podepsaný certifikát pro uzel Connect:Direct .

   To můžete provést pomocí nástroje IBM Správa klíčů, který je poskytován s produktem IBM MQ. Další informace viz téma “Práce s SSL/TLS” na stránce 276.
2. Odešlete žádost certifikační autoritě o podepsání klíče. Obdržíte certifikát na oplátku.
3. Vytvořte textový soubor, například `/test/ssl/certs/CAcert`, který obsahuje veřejný klíč vaší certifikační autority.
4. Nainstalujte volbu Secure + na uzel Connect:Direct .

   Pokud uzel již existuje, můžete nainstalovat volbu Secure + Option opětovným spuštěním instalačního programu, uvedením umístění existující instalace a výběrem instalace pouze volby Secure + Option.
5. Vytvořte nový textový soubor, například `/test/ssl/cd/keyCertFile/`*`node_name`*`.txt`.
6. Zkopírujte certifikát, který jste obdrželi od certifikační autority, a soukromý klíč umístěný v adresáři `/test/ssl/cd/privateKeys/`*`node_name`*`.key`do textového souboru.

   Obsah souboru `/test/ssl/cd/keyCertFile/`*`node_name`*`.txt` musí být v následujícím formátu:

```
-----BEGIN CERTIFICATE-----
MIICnzCCAgigAwIBAgIBGjANBgkqhkiG9w0BAQUFADBeMQswCQYDVQQGEwJHQjES
MBAGA1UECBMJSGFtcHNoaXJlMRAwDgYDVQQHEwdIdXJzbGV5MQwwCgYDVQQKEwNJ
Qk0xDjAMBgNVBAsTBU1RSVBUMQswCQYDVQQDEwJDQTAeFw0xMTAzMDExNjIwNDZa
Fw0yMTAyMjYxNjIwNDZaMFAxCzAJBgNVBAYTAkdCMRIwEAYDVQQIEwlIYW1wc2hp
cmUxDDAKBgNVBAoTA0lCTTEOMAwGA1UECxMFTVFGVEUxDzANBgNVBAMTBmJpbmJh
ZzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAvgP1QIklU9ypSKD1XoODo1yk
EyMFXBOUpZRrDVxjoSEC0vtWNcJ199e+Vc4UpNybDyBu+NkDlMNofX4QxeQcLAFj
WnhakqCiQ+JIAD5AurhnrwChe0MV3kjA84GKH/rOSVqtl984mu/lDyS819XcfSSn
cOOMsK1KbneVSCIV2XECAwEAAaN7MHkwCQYDVR0TBAIwADAsBglghkgBhvhCAQ0E
HxYdT3BlblNTTCBHZW5lcmF0ZWQgQ2VydGlmaWNhdGUwHQYDVR0OBBYEFNXMIpSc
csBXUniW4A3UrZnCRsv3MB8GA1UdIwQYMBaAFDXY8rmj4lVz5+FVAoQb++cns+B4
MA0GCSqGSIb3DQEBBQUAA4GBAFc7klXa4pGKYgwchxKpE3ZF6FNwy4vBXS216/ja
```

```
8h/vl8+iv01OCL8t0ZOKSU95fyZLzOPKnCH7v+ItFSE3CIiEk9Dlz2U6WO9lICwn
l7PL72TdfaL3kabwHYVf17IVcuL+VZsZ3HjLggP2qHO9ZuJPspeT9+AxFVMLiaAb
8eHw
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,64A02DA15B6B6EF9

57kqxLOJ/gRUOIQ6hVK2YN13B4E1jAi1gSme0I5ZpEIG8CHXISKB7/0cke2FTqsV
lvI99QyCxsDWoMNt5fj51v7aPmVeS60bOm+UlGre8B/Ze18JVj2O4K2Uh72rDCXE
5e6eFxSdUM207sQDy20euBVELJtM2kOkL1ROdoQQSlU3XQNgJw/t3ZIx5hPXWEQT
rjRQO64BEhb+PzzxPF8uwzZ9IrUK9BJ/UUnqC6OdBR87IeA4pnJD1Jvb2ML7EN9Z
5Y+50hTKI8OGvBvWXO4fHyvIX5as1whBoArXIS1AtNTrptPvoaP1zyIAeZ6OCVo/
SFo+A2UhmtEJeOJaZG2XZ3H495fAw/EHmjehzIACwukQ9nSIETgu4A1+CV64RJED
aYBCM8UjaAkbZDH5gn7+eBov0ssXAXWDyJBVhUOjXjvAj/e1h+kcSF1hax5D//AI
66nRMZzboSxNqkjcVd8wfDwP+bEjDzUaaarJTS7lIFeLLw7eJ8MNAkMGicDkycL0
EPBU9X5QnHKLKOfYHN/1WgUk8qt3UytFXXfzTXGF3EbsWbBupkT5e5+lYcX8OVZ6
sHFPNlHluCNy/riUcBy9iviVeodX8IomOchSyO5DKl8bwZNjYtUP+CtYHNFU5BaD
I+1uUOAeJ+wjQYKT1WaeIGZ3VxuNITJul8y5qDTXXfX7vxM5OoWXa6U5+AYuGUMg
/itPZmUmNrHjTk7ghT6i1IQOaBowXXKJBlMmq/6BQXN2IhkD9ys2qrvM1hdi5nAf
egmdiG50loLnBRqWbfR+DykpAhK4SaDi2F52Uxovw3Lhiw8dQP7lzQ==
-----END RSA PRIVATE KEY-----
```

7. Spusťte nástroj Secure + Admin Tool.
   - Na systémech AIX and Linux spusťte příkaz **spadmin.sh**.
   - V systémech Windows klepněte na volbu **Spustit** > **Programy** > **Sterling Commerce Connect:Direct** > **CD Secure + Admin Tool**

   Spustí se nástroj CD Secure + Admin Tool.
8. V nástroji CD Secure + Admin Tool poklepejte na soubor **.Lokální řádek** pro úpravu hlavního nastavení SSL nebo TLS.
   a) V závislosti na používaném protokolu vyberte volbu **Povolit protokol SSL** nebo **Povolit protokol TLS**.
   b) Vyberte volbu **Zakázat přepis**.
   c) Vyberte alespoň jednu sadu Cipher Suite.
   d) Chcete-li obousměrné ověření, změňte hodnotu **Povolit ověření klienta** na Yes.
   e) Do pole **Důvěryhodný kořenový certifikát** zadejte cestu k veřejnému souboru certifikátů vaší certifikační autority `/test/ssl/certs/CAcert`.
   f) Do pole **Soubor s certifikátem klíče** zadejte cestu k souboru, který jste vytvořili, `/test/ssl/cd/keyCertFile/`*node_name*`.txt`.
9. Poklepejte na soubor **.Řádek klienta** pro úpravu hlavního nastavení SSL nebo TLS.
   a) V závislosti na používaném protokolu vyberte volbu **Povolit protokol SSL** nebo **Povolit protokol TLS**.
   b) Vyberte volbu **Zakázat přepis**.

V případě agenta mostu Connect:Direct postupujte takto:

10. Vytvořte úložiště údajů o důvěryhodnosti. Můžete to provést vytvořením fiktivního klíče a následným odstraněním fiktivního klíče.

    Můžete použít následující příkazy:

```
keytool -genkey -alias dummy -keystore /test/ssl/fte/stores/truststore.jks
```

```
keytool -delete -alias dummy -keystore /test/ssl/fte/stores/truststore.jks
```

11. Importujte veřejný certifikát certifikační autority do úložiště údajů o důvěryhodnosti.

    Můžete použít následující příkaz:

```
keytool -import -trustcacerts -alias myCA
        -file /test/ssl/certs/CAcert
        -keystore /test/ssl/fte/stores/truststore.jks
```

12. Upravte soubor vlastností agenta mostu Connect:Direct .

    Zahrňte následující řádky kdekoli v souboru:

    ```
    cdNodeProtocol=protocol
    cdNodeTruststore=/test/ssl/fte/stores/truststore.jks
    cdNodeTruststorePassword=password
    ```

    V příkladu v tomto kroku je *protokol* protokol, který používáte, buď SSL, nebo TLS, a *heslo* je heslo, které jste zadali při vytváření úložiště údajů o důvěryhodnosti.
13. Chcete-li obousměrné ověření, vytvořte klíč a certifikát pro agenta mostu Connect:Direct .

    a) Vytvořte úložiště klíčů a klíč.

    Můžete použít následující příkaz:

    ```
    keytool -genkey -keyalg RSA -alias agent_name
            -keystore /test/ssl/fte/stores/keystore.jks
            -storepass password -validity 365
    ```

    b) Vygenerujte požadavek na podepsání.

    Můžete použít následující příkaz:

    ```
    keytool -certreq -v -alias agent_name
            -keystore /test/ssl/fte/stores/keystore.jks -storepass password
            -file /test/ssl/fte/requests/agent_name.request
    ```

    c) Importujte certifikát, který jste obdrželi z předchozího kroku, do úložiště klíčů. Certifikát musí být ve formátu x.509 .

    Můžete použít následující příkaz:

    ```
    keytool -import -keystore /test/ssl/fte/stores/keystore.jks
            -storepass password -file certificate_file_path
    ```

    d) Upravte soubor vlastností agenta mostu Connect:Direct .

    Zahrňte následující řádky kdekoli v souboru:

    ```
    cdNodeKeystore=/test/ssl/fte/stores/keystore.jks
    cdNodeKeystorePassword=password
    ```

    V příkladu v tomto kroku je *heslo* heslo, které jste zadali při vytváření úložiště klíčů.

Související úlohy

Konfigurace mostu Connect:Direct

ALW Zabezpečení klientů AMQP

K zabezpečení připojení od klientů AMQP a k zajištění vhodné ochrany dat v síti používáte celou řadu bezpečnostních mechanismů. Zabezpečení můžete sestavit do svých aplikací MQ Light . Můžete také použít existující funkce zabezpečení produktu IBM MQ s klienty AMQP stejným způsobem, jako se tyto funkce používají pro jiné aplikace.

Pravidla ověřování kanálu (CHLAUTH)

Pomocí pravidel ověřování kanálu můžete omezit připojení TCP ke správci front. Kanály AMQP podporují použití pravidel ověřování kanálu, která konfigurujete pro správce front. Jsou-li definována pravidla ověřování kanálu s profilem, který odpovídá libovolným kanálům AMQP ve vašem správci front, budou tato pravidla pro tyto kanály použita. Při výchozím nastavení je ověřování kanálu povoleno pro nové správce front produktu IBM® MQ , takže před použitím kanálu AMQP je třeba provést alespoň určitou konfiguraci.

Další informace o konfiguraci pravidel ověřování kanálu tak, aby umožňovala připojení AMQP ke správci front, naleznete v tématu Vytvoření a použití kanálů AMQP.

Ověření připojení (CONNAUTH)

K ověřování připojení ke správci front lze použít ověřování připojení. Kanály AMQP podporují použití ověřování připojení k řízení přístupu ke správci front z aplikací AMQP.

Protokol AMQP používá rámec SASL (Simple Authentication and Security Layer) k určení způsobu ověřování připojení. Existují různé mechanismy SASL a IBM MQ podporuje dva mechanismy SASL: ANONYMOUS a PLAIN.

V případě ANONYMOUS nejsou z klienta do správce front předána žádná pověření k ověření. Pokud má objekt MQ AUTHINFO určený v atributu CONNAUTH hodnotu CHCKCLNT REQUIRED nebo REQDADM (pokud se připojujete jako administrativní uživatel), bude připojení odmítnuto. Je-li hodnota CHCKCLNT NONE nebo OPTIONAL, bude připojení přijato.

V případě PLAIN je jméno uživatele a heslo předáno z klienta do správce front k ověření. Pokud má objekt MQ AUTHINFO určený v atributu CONNAUTH hodnotu CHCKCLNT NONE, bude připojení odmítnuto. Je-li hodnota CHCKCLNT OPTIONAL, REQUIRED nebo REQDADM (pokud se připojujete jako administrativní uživatel), je jméno uživatele a heslo kontrolováno správcem front. Správce front kontroluje operační systém (pokud je objekt AUTHINFO typu IDPWOS) nebo úložiště LDAP (pokud je objekt AUTHINFO typu IDPWLDAP).

Následující tabulka shrnuje toto chování ověření:

Tabulka 102. Souhrn mechanizmů SASL a ověřování připojení

Mechanizmus SASL	**Pověření předaná z klienta do správce front?**	**Hodnota CHKCLNT**
anonymní	Ne	REQUIRED nebo REQDADM-spojení odmítnuto NONE nebo OPTIONAL-připojení je akceptováno
Prostý	Ano, jméno uživatele a heslo	REQUIRED, REQDADM nebo OPTIONAL-jméno uživatele a heslo kontrolované správcem front NONE-připojení odmítnuto

Pokud používáte klienta MQ Light , můžete zadat pověření jejich zahrnutím do adresy AMQP, ke které se připojujete, například:

```
amqp://mwhitehead:mYp4ssw0rd@localhost:5672/sports/football
```

Nastavení MCAUSER na kanálu

Kanály AMQP mají atribut MCAUSER, který můžete použít k nastavení ID uživatele IBM MQ , pod kterým jsou autorizována všechna připojení k tomuto kanálu. Všechna připojení z klientů AMQP k tomuto kanálu přebírají ID MCAUSER, které jste nakonfigurovali. Toto ID uživatele se používá pro autorizaci systému zpráv v různých tématech.

K zabezpečení připojení ke správcům front se doporučuje použít ověřování kanálu (CHLAUTH). Používáte-li ověřování kanálu, doporučuje se konfigurovat hodnotu MCAUSER pro neprivilegovaného uživatele. Tím

je zajištěno, že pokud připojení ke kanálu neodpovídá pravidlu CHLAUTH, není připojení autorizováno k provádění žádného systému zpráv ve správci front.

Poznámka: Windows V systému Windowspřed IBM MQ 9.2je nastavení ID uživatele MCAUSER podporováno pouze pro ID uživatelů s délkou nejvýše 12 znaků. Od verze IBM MQ 9.2Long Term Support již neplatí limit délky max. 12 znaků.

Podpora SSL/TLS

Kanály APMQP podporují šifrování SSL/TLS pomocí klíčů z úložiště klíčů konfigurovaného pro vašeho správce front. Volby konfigurace kanálu AMQP pro šifrování SSL/TLS podporují stejné volby jako jiné typy kanálu produktu MQ . Můžete určit specifikaci šifry a určit, zda správce front vyžaduje certifikáty od připojení klienta AMQP.

Pomocí atributů FIPS správce front můžete řídit šifrovací sady SSL/TLS, které můžete použít k zabezpečení připojení od klientů AMQP.

Informace o nastavení úložiště klíčů pro správce front viz “Práce se zabezpečením SSL/TLS v systému AIX, Linux, and Windows” na stránce 293.

Informace o konfiguraci podpory SSL/TLS pro připojení klienta AMQP naleznete v tématu Vytvoření a použití kanálů AMQP.

Java Služba ověřování a autorizace (JAAS)

Volitelně můžete nakonfigurovat kanály AMQP pomocí přihlašovacího modulu JAAS , který může zkontrolovat jméno uživatele a heslo poskytnuté klientem AMQP. Viz “Konfigurace JAAS pro kanály AMQP” na stránce 612.

Související úlohy

Vývoj klientských aplikací AMQP

Vytváření a používání kanálů AMQP

ALW Omezení převzetí klienta AMQP

Když se vytvoří připojení klienta AMQP, které má stejný identifikátor klienta jako existující připojení klienta AMQP, existující připojení klienta se standardně odpojí. Správce front však můžete nakonfigurovat tak, aby omezoval chování klienta při převzetí, takže převzetí je možné pouze v případě, že jsou splněna určitá kritéria.

Například odpojení existujícího připojení klienta nemusí být vhodné, pokud existují aplikace AMQP vyvíjené různými týmy a používají stejné ID klienta. Chcete-li tento problém vyřešit, můžete omezit převzetí klienta na základě názvu používaného kanálu AMQP, adresy IP klienta a ID uživatele klienta (je-li povoleno ověření SASL).

Pomocí nastavení atributů správce front **AdoptNewMCA** a **AdoptNewMCACheck** můžete určit požadovanou úroveň omezení převzetí klienta, jak je podrobně popsáno v následující tabulce:

*Tabulka 103. Nastavení **AdoptNewMCA** a **AdoptNewMCACheck** pro omezení převzetí klienta*

AdoptNewMCA	AdoptNewMCACheck	Kritéria zaškrtnutá před povolením převzetí klienta
NO nebo nedefinováno	Nelze použít	Není. Převzetí klienta je povoleno pro všechna připojení klienta, která jsou ověřena a předávají všechna pravidla CHLAUTH.
ALL (nebo hodnota jiná než NO)	QM nebo nedefinované	Není. Převzetí klienta je povoleno pro všechna připojení klienta, která jsou ověřena a předávají všechna pravidla CHLAUTH.

*Tabulka 103. Nastavení **AdoptNewMCA** a **AdoptNewMCACheck** pro omezení převzetí klienta (pokračování)*		
AdoptNewMCA	**AdoptNewMCACheck**	**Kritéria zaškrtnutá před povolením převzetí klienta**
ALL (nebo hodnota jiná než NO)	NÁZEV	ID uživatele (při povolení SASL) Název kanálu
ALL (nebo hodnota jiná než NO)	ADDRESS	ID uživatele (při povolení SASL) Adresa IP
ALL (nebo hodnota jiná než NO)	ALL	ID uživatele (při povolení SASL) Název kanálu Adresa IP

Atributy správce front **AdoptNewMCA** a **AdoptNewMCACheck** jsou součástí konfigurace správce front, která je definována v sekci CHANNELS. V systémech IBM MQ for Windows a IBM MQ for Linux x86-64 upravte informace o konfiguraci pomocí konzoly IBM MQ Explorer. Na jiných systémech upravte informace úpravou konfiguračního souboru `qm.ini` . Informace o úpravě informací o kanálech správce front naleznete v tématu Atributy kanálů.

Související úlohy

Vývoj klientských aplikací AMQP

Vytváření a používání kanálů AMQP

ALW Konfigurace JAAS pro kanály AMQP

Vlastní moduly služby Java Authentication and Authorization Service (JAAS) lze použít k ověření pověření jména uživatele a hesla předaných kanálu AMQP klientem AMQP při připojení.

Informace o této úloze

Můžete použít vlastní modul JAAS , pokud již používáte moduly JAAS pro ověřování v jiných systémech založených na systému Javaa chcete tyto moduly znovu použít pro ověřování připojení AMQP k produktu MQ. Případně můžete napsat vlastní modul JAAS , pokud funkce ověřování vestavěné do produktu MQ nepodporují mechanizmus ověřování, který chcete použít.

Konfigurace modulů JAAS pro kanály AMQP se provádí na úrovni správce front. To znamená, že pokud nakonfigurujete modul JAAS pro ověřování připojení AMQP ke správci front, bude modul platit pro všechny kanály AMQP. Název kanálu, který vyvolal modul JAAS , je předán modulu, což umožňuje kódovat různé chování přihlášení JAAS pro různé kanály.

Další informace jsou předány také modulu JAAS :

- ID klienta AMQP, který se pokouší ověřit.
- Síťová adresa klienta AMQP.
- Název kanálu, který vyvolal modul JAAS .

Postup

Konfigurujte konfigurační modul JAAS pro kanály AMQP provedením následujících kroků:

1. Definujte soubor `jaas.config` obsahující jednu nebo více sekcí konfigurace modulu JAAS . Sekce musí uvádět úplný název třídy Java , která implementuje rozhraní JAAS `javax.security.auth.spi.LoginModule` .
   - Výchozí soubor `jaas.config` je dodáván s produktem a je umístěn v adresáři *QM_data_directory*/amqp/jaas.config.

- Předkonfigurovaná sekce s názvem `MQXRConfig` je již definována ve výchozím souboru `jaas.config` .

2. Uveďte název sekce, která se má použít pro kanály AMQP.
   - Linux AIX Přidejte vlastnost do souboru `amqp_unix.properties` .
   - Windows Přidejte vlastnost do souboru `amqp_win.properties` .

   Vlastnost má následující formu:

   ```
   com.ibm.mq.MQXR.JAASConfig=JAAS_stanza_name
   ```

   Příklad:

   ```
   com.ibm.mq.MQXR.JAASConfig=MQXRConfig
   ```

3. Nakonfigurujte prostředí správce front tak, aby obsahovalo třídu vlastního modulu. Služba AMQP musí mít přístup ke třídě Java nakonfigurované v sekci konfigurace JAAS .

   To provedete přidáním cesty ke třídě JAAS do souboru MQ `service.env` . Upravte soubor `service.env` v konfiguračním adresáři produktu MQ (*MQ_config_directory*) nebo v konfiguračním adresáři správce front (*QM_config_directory*) a nastavte proměnnou CLASSPATH na umístění třídy modulu JAAS .

Jak pokračovat dále

Ukázkový přihlašovací modul JAAS je dodáván s produktem v adresáři *mq_installation_directory*/amqp/samples . Ukázkový přihlašovací modul JAAS ověřuje všechna připojení klienta bez ohledu na jméno uživatele nebo heslo, ke kterému se klient připojuje.

Můžete upravit zdrojový kód ukázky a znovu jej zkompilovat, abyste se pokusili ověřit pouze specifické uživatele s konkrétním heslem. Chcete-li nakonfigurovat kanál AMQP v systému UNIX tak, aby používal ukázkový přihlašovací modul JAAS dodávaný s produktem, postupujte takto:

1. Upravte soubor `/var/mqm/qmgrs/QMNAME/amqp/amqp_unix.properties` a nastavte vlastnost `com.ibm.mq.MQXR.JAASConfig=MQXRConfig`.
2. Upravte soubor /var/mqm/service.env a nastavte vlastnost `CLASSPATH=`*mq_installation_location*`/amqp/samples` .

Soubor `jaas.config` již obsahuje sekci s názvem `MQXRConfig` , která uvádí ukázkovou třídu `samples.JAASLoginModule` jako třídu přihlašovacího modulu. Před tím, než se pokusíte o ukázkový modul, nejsou v produktu `jaas.config` vyžadovány žádné změny.

Související úlohy

Vývoj klientských aplikací AMQP

Vytváření a používání kanálů AMQP

Advanced Message Security

Advanced Message Security (AMS) je komponenta produktu IBM MQ , která poskytuje vysokou úroveň ochrany citlivých dat procházejících sítí IBM MQ , aniž by to mělo vliv na koncové aplikace.

Přehled produktu Advanced Message Security

Aplikace IBM MQ mohou používat produkt Advanced Message Security k odesílání citlivých dat, jako jsou finanční transakce s vysokou hodnotou a osobní informace, s různými úrovněmi ochrany pomocí modelu šifrování s veřejným klíčem.

Související pojmy

“Zachycení agenta MCA (Message Channel Agent) a AMS” na stránce 664

Zachycení MCA umožňuje správci front spuštěnému v adresáři IBM MQ selektivně povolit použití zásad pro kanály připojení serveru.

Související odkazy

IBM Global Security Kit (GSKit) návratové kódy použité ve zprávách AMS

Vlastnosti a funkce produktu Advanced Message Security

Advanced Message Security rozšiřuje IBM MQ služby zabezpečení tak, aby poskytovaly podepisování a šifrování dat na úrovni zpráv. Rozšířené služby zaručují, že data zpráv nebyla změněna mezi tím, kdy byla původně umístěna do fronty, a tím, kdy byla načtena. Kromě toho produkt AMS ověřuje, zda je odesilatel dat zprávy autorizován k umístění podepsaných zpráv do cílové fronty.

Produkt AMS poskytuje následující funkce:

- Zabezpečuje citlivé transakce nebo transakce s vysokou hodnotou zpracované produktem IBM MQ.
- Detekuje a odstraňuje nepoctiví nebo neoprávněné zprávy před tím, než jsou zpracovány přijímací aplikace.
- Ověřuje, zda během přenosu zpráv z fronty do fronty nebyly změněny.
- Chrání data nejen při toku po síti, ale i při vložení do fronty.
- Zabezpečuje existující proprietární a zákazníkem psané aplikace pro IBM MQ.
- z/OS V produktu IBM MQ 9.1.3poskytuje produkt IBM MQ for z/OS možnost volitelně odebrat a přidat ochranu AMS ze zpráv nebo do zpráv, které proudí po síti. Toto je známé jako *Server to Server Message Channel Agent (MCA) Interception.*.
- ALW V produktu IBM MQ 9.1.4 a IBM MQ 9.1.0 Fix Pack 4je do kódu knihovny IBM MQ přidána kontrola, která se spouští v rámci aplikačního programu zákazníka. Kontrola se spustí v rané fázi inicializace, aby se přečetla hodnota proměnné prostředí *AMQ_AMS_FIPS_OFF* , a pokud je nastavena na libovolnou hodnotu, spustí se kód IBM Global Security Kit (GSKit) v této aplikaci v režimu jiném než FIPS.

Kvalita ochrany k dispozici s AMS

Existují tři kvality ochrany pro Advanced Message Security, `Integrity`, `Privacy`a `Confidentiality`.

Ochrana systému `Integrity` je poskytována digitálním podpisem, který zajišťuje, kdo zprávu vytvořil, a že zpráva nebyla pozměněna nebo s ní nebylo manipulováno.

Ochrana systému `Privacy` je zajištěna kombinací digitálního podepisování a šifrování. Šifrování zajistí, že data zprávy budou zobrazitelná pouze zamýšlenému příjemci nebo příjemcům. I když neautorizovaní příjemci získají kopii šifrovaných dat zprávy, nejsou schopni zobrazit skutečná data zprávy sami.

Ochrana systému `Confidentiality` je poskytována šifrováním pouze s volitelným opětovným použitím klíče.

Vliv na výkon

Produkt AMS používá k zajištění digitálního podepisování a šifrování kombinaci symetrických a asymetrických šifrovacích rutin. Vzhledem k tomu, že symetrické klíčové operace jsou velmi rychlé ve srovnání s asymetrickými klíčovými operacemi, které jsou náročné na CPU, může to mít významný dopad na náklady na ochranu velkého počtu zpráv pomocí produktu AMS.

Asymetrické šifrovací rutiny

Například při vkládání podepsané zprávy je hašování zprávy podepsáno pomocí operace asymetrického klíče.

Při získávání podepsané zprávy se k ověření podepsaného hašování použije další operace asymetrického klíče.

Proto jsou pro podepsání a ověření dat zprávy vyžadovány minimálně dvě asymetrické klíčové operace na jednu zprávu.

Asymetrické a symetrické šifrovací rutiny

Při vkládání šifrované zprávy se vygeneruje symetrický klíč a poté se zašifruje pomocí operace asymetrického klíče pro každého zamýšleného příjemce zprávy.

Data zprávy jsou pak zašifrována pomocí symetrického klíče. Při získávání šifrované zprávy musí příjemce použít operaci asymetrického klíče, aby zjistil symetrický klíč používaný pro zprávu.

Všechny tři kvality ochrany proto obsahují různé prvky operací s intenzivním asymetrickým klíčem CPU, což bude mít významný dopad na maximální dosažitelnou rychlost zasílání zpráv pro aplikace, které vkládají a získávají zprávy.

Zásady systému `Confidentiality` však umožňují opakované použití symetrických klíčů v posloupnosti zpráv. Výrazné úspory nákladů na procesor lze dosáhnout pomocí zásad `Confidentiality` pomocí symetrického opětovného použití klíče. Tento režim operace i nadále používá formát PKCS#7 ke sdílení symetrického šifrovacího klíče. Neexistuje však žádný digitální podpis, který by eliminoval některé operace s asymetrickým klíčem pro každou zprávu. Symetrický klíč stále musí být šifrován pomocí operací asymetrického klíče pro každého příjemce, ale symetrický klíč může být volitelně znovu použit pro více zpráv, které jsou určeny pro stejné příjemce. Pokud zásada povoluje opětovné použití klíče, pak pouze první zpráva vyžaduje operace s asymetrickým klíčem. Následné zprávy musí používat pouze operace symetrického klíče.

Opětovné použití klíče

Pomocí zásad `Confidentiality` můžete použít přístup symetrického opětovného použití klíče k výraznému snížení nákladů spojených s šifrováním řady zpráv, které jsou vloženy do stejné fronty a určeny pro stejného příjemce nebo příjemce.

Například při vložení 10 šifrovaných zpráv do stejné sady příjemců se vygeneruje symetrický klíč a pak se zašifruje pro první zprávu pomocí operace asymetrického klíče pro každého zamýšleného příjemce zprávy.

Na základě omezení řízených zásadou může být zašifrovaný symetrický klíč znovu použit následnými zprávami, které jsou určeny pro stejné příjemce. Aby mohl být symetrický klíč znovu použit následnými zprávami, musí aplikace po vložení zprávy do fronty ponechat frontu otevřenou. Symetrický klíč nelze znovu použít operacemi MQPUT1 . Aplikace, která získává šifrované zprávy, může použít stejnou optimalizaci v tom, že může zjistit, kdy se symetrický klíč nezměnil, a vyhnout se nákladům na načtení symetrického klíče.

V tomto příkladu se lze vyhnout 90% operací asymetrického klíče, a to jak při vkládání, tak při získávání aplikací opětovným použitím stejného klíče.

Další informace o tom, jak používat opětovné použití klíče, viz:

- Příkaz MQSC SET POLICY
- Řídicí příkaz setmqspl
- IBM i IBM i příkaz SETMQMSPL

Klíčové koncepty v produktu AMS

Seznamte se s klíčovými koncepty v produktu Advanced Message Security , abyste pochopili, jak nástroj funguje a jak jej efektivně spravovat.

Infrastruktura veřejných klíčů a Advanced Message Security

Infrastruktura veřejných klíčů (PKI) je systém zařízení, zásad a služeb, které podporují použití šifrování veřejných klíčů k získání zabezpečené komunikace.

Neexistuje jediný standard, který by definoval komponenty infrastruktury veřejných klíčů, ale infrastruktura PKI obvykle zahrnuje použití certifikátů veřejných klíčů a zahrnuje certifikační autority (CA) a další registrační orgány (RA), které poskytují následující služby:

- Vydávání digitálních certifikátů
- Ověření digitálních certifikátů

- Odvolání digitálních certifikátů
- Distribuce certifikátů

Identita uživatelů a aplikací je reprezentována polem **rozlišující název (DN)** v certifikátu přidruženém k podepsaným nebo šifrovaným zprávám. Produkt Advanced Message Security používá tuto identitu k reprezentaci uživatele nebo aplikace. Chcete-li ověřit tuto identitu, musí mít uživatel nebo aplikace přístup k úložišti klíčů, kde je uložen certifikát a přidružený soukromý klíč. Každý certifikát je v úložišti klíčů reprezentován popiskem.

Související pojmy

“Použití úložišť klíčů a certifikátů s produktem AMS” na stránce 657
K zajištění transparentní kryptografické ochrany pro aplikace IBM MQ používá produkt Advanced Message Security soubor úložiště klíčů, ve kterém jsou uloženy certifikáty veřejného klíče a soukromý klíč. V systému z/OSse místo souboru úložiště klíčů používá svazek klíčů SAF.

Digitální certifikáty v AMS

Produkt Advanced Message Security přidružuje uživatele a aplikace ke standardním digitálním certifikátům X.509 . Certifikáty X.509 jsou obvykle podepsány důvěryhodnou certifikační autoritou (CA) a zahrnují soukromé a veřejné klíče, které se používají pro šifrování a dešifrování.

Digitální certifikáty poskytují ochranu před zosobněním prostřednictvím vazby veřejného klíče na jeho vlastníka, ať už je tento vlastník jednotlivec, správce front nebo jiná entita. Digitální certifikáty jsou také známé jako certifikáty veřejných klíčů, protože vám poskytují záruku vlastnictví veřejného klíče, když používáte schéma asymetrického klíče. Toto schéma vyžaduje, aby byl pro aplikaci vygenerován veřejný a soukromý klíč. Data zašifrovaná pomocí veřejného klíče lze dešifrovat pouze pomocí odpovídajícího soukromého klíče, zatímco data zašifrovaná pomocí soukromého klíče lze dešifrovat pouze pomocí odpovídajícího veřejného klíče. Soukromý klíč je uložen v souboru databáze klíčů, který je chráněn heslem. Pouze jeho vlastník má přístup k soukromému klíči použitému k dešifrování zpráv, které jsou šifrovány pomocí odpovídajícího veřejného klíče.

Pokud jsou veřejné klíče odesílány přímo jejich vlastníkem jiné entitě, existuje riziko, že by mohla být zpráva zachycena a veřejný klíč nahrazen jiným. To je známé jako "man-in-the-middle" útok. Řešením je výměna veřejných klíčů prostřednictvím důvěryhodné třetí strany, což uživateli poskytuje silnou záruku, že veřejný klíč patří k subjektu, se kterým komunikujete. Místo toho, abyste veřejný klíč odeslali přímo, požádejte důvěryhodnou třetí stranu, aby jej začlenila do digitálního certifikátu. Důvěryhodná třetí strana, která vydává digitální certifikáty, se nazývá certifikační autorita (CA).

Další informace o digitálních certifikátech naleznete v tématu Co je v digitálním certifikátu.

Digitální certifikát obsahuje veřejný klíč pro entitu a uvádí, že veřejný klíč patří této entitě:

- když je certifikát určen pro jednotlivou entitu, nazývá se *osobní certifikát* nebo *uživatelský certifikát*.
- když je certifikát určen pro certifikační autoritu, nazývá se certifikát *certifikátem CA* nebo *certifikátem podepsaného*.

Poznámka: Produkt Advanced Message Security podporuje certifikáty podepsané svým držitelem v produktu Java i v nativních aplikacích.

Související pojmy

“Šifrování” na stránce 11
Šifrování je proces převodu mezi čitelným textem, který se nazývá *prostý text*, a nečitelnou formou, která se nazývá *šifrovaný text*.

Multi *Správce oprávnění k objektu a AMS*

Na platformě Multiplatforms je OAM (Object Authority Manager) komponenta služby autorizace dodávaná s produkty IBM MQ .

Přístup k entitám Advanced Message Security je řízen prostřednictvím skupin uživatelů IBM MQ a OAM. Administrátoři mohou použít rozhraní příkazového řádku k udělení nebo zrušení oprávnění podle potřeby. Různé skupiny uživatelů mohou mít různé druhy přístupových oprávnění ke stejným objektům. Například jedna skupina může provádět operace PUT i GET pro specifickou frontu, zatímco jiná skupina může mít

povoleno pouze procházet frontu. Podobně některé skupiny mohou mít oprávnění GET a PUT k frontě, ale nemohou frontu měnit nebo odstranit.

Prostřednictvím OAM můžete ovládat:

- Přístup k objektům Advanced Message Security prostřednictvím rozhraní MQI (Message Queue Interface). Když se aplikační program pokusí o přístup k objektům, OAM zkontroluje, zda má profil uživatele, který zadal požadavek, oprávnění pro požadovanou operaci. To znamená, že fronty a zprávy ve frontách mohou být chráněny před neoprávněným přístupem.
- Oprávnění k použití příkazů PCF a MQSC.

Související pojmy

Správce oprávnění k objektu

Přehled rozhraní fronty zpráv

Technologie podporovaná společností Advanced Message Security

Produkt Advanced Message Security závisí na několika technologických komponentách, které poskytují infrastrukturu zabezpečení.

Produkt Advanced Message Security podporuje následující rozhraní API produktu IBM MQ :

- Message Queue Interface (MQI)
- IBM MQ Java Message Service (JMS) 1.0.2 a 1.1.
- IBM MQ Základní třídy pro Java
- Třídy IBM MQ pro. Net v nespravovaném režimu

Poznámka: Produkt Advanced Message Security podporuje certifikační autority kompatibilní s X.509 .

Známá omezení AMS

Existuje řada voleb IBM MQ , které buď nejsou podporovány, nebo mají omezení pro Advanced Message Security.

- Následující volby IBM MQ nejsou podporovány nebo mají omezení:

  Publikování/odběr
  Jedním z hlavních přínosů modelu systému zpráv publikování/odběru přes dvoubodový systém je to, že odesílající a přijímající aplikace nemusí vědět nic o sobě pro data, která mají být odeslána a přijata. Tento přínos je negován použitím zásad Advanced Message Security , které musí definovat zamýšlené příjemce nebo oprávněné podepisující subjekty. Je možné, aby aplikace publikovala do tématu prostřednictvím definice alias fronty, která je chráněna zásadou, je také možné, aby odebírající aplikace získala zprávy z fronty chráněné zásadou. Není možné přiřadit zásadu přímo k řetězci tématu, zásady lze přiřadit pouze k definicím fronty.

  Převod dat kanálu
  Chráněný informační obsah zprávy chráněné produktem Advanced Message Security je přenášen pomocí binárního formátu, což zajišťuje, že převod dat na kanálu mezi aplikacemi nezruší platnost kódu digest zprávy. Aplikace, které načítají zprávy z fronty chráněné zásadou, by měly požadovat převod dat, po úspěšném ověření a nechránění zpráv bude proveden pokus o převod chráněného informačního obsahu.

  Distribuční seznamy
  Zásady produktu Advanced Message Security lze použít při ochraně aplikací, které vkládají zprávy do distribučních seznamů, za předpokladu, že každá cílová fronta v seznamu má definovanou identickou zásadu. Pokud jsou při otevření distribučního seznamu aplikací identifikovány nekonzistentní zásady, operace otevření selže a aplikaci se vrátí chyba zabezpečení.

  Segmentace zpráv aplikace
  Velikost zpráv chráněných zásadou se zvýší a není možné, aby aplikace přesně určily hranice segmentu zprávy.

Aplikace používající produkt IBM MQ classes for .NET ve spravovaném režimu (připojení klienta)
Aplikace používající produkt IBM MQ classes for .NET ve spravovaném režimu (připojení klienta) nejsou podporovány.

Poznámka: Zachycení MCA lze použít, aby nepodporovaní klienti mohli používat AMS.

Klient služby zpráv pro aplikace .NET (XMS) ve spravovaném režimu
Klient služby zpráv pro aplikace .NET (XMS) ve spravovaném režimu není podporován.

Poznámka: Zachycení MCA lze použít k tomu, aby nepodporovaní klienti mohli používat AMS.

IBM MQ front zpracovaných mostem IMS
Fronty IBM MQ zpracované mostem IMS nejsou podporovány.

Poznámka: Produkt AMS je podporován ve frontách mostu CICS . Pro MQPUT (encrypt) a MQGET (decrypt) ve frontách mostu CICS byste měli použít stejné ID uživatele.

Vložit do čekající metody getter
Vložení do čekající metody getter není podporováno pro aplikace getter pro fronty, pro které jsou definovány zásady AMS .

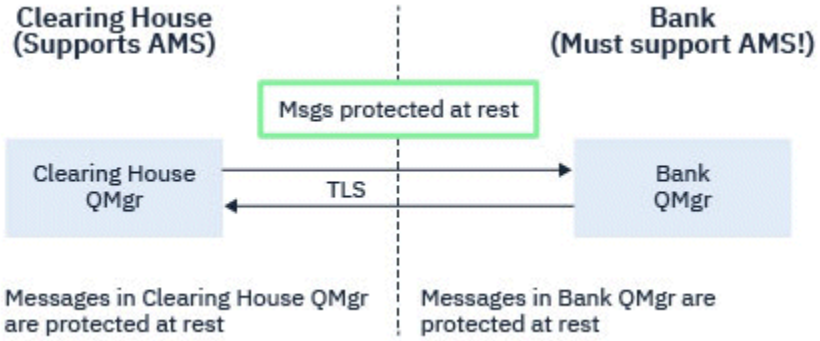
Zachycení MCA ze serveru na server
Z produktu IBM MQ for z/OS 9.1.3je zachycení MCA mezi servery podporováno pouze pro typy kanálů odesilatel, server, příjemce a žadatel.

- Uživatelé by se měli vyvarovat vložení více než jednoho certifikátu se stejným rozlišujícím názvem do jednoho souboru úložiště klíčů, protože volba, který certifikát se má použít při ochraně zprávy, není definována.
- Parametr AMS není v produktu JMS podporován, pokud je vlastnost **WMQ_PROVIDER_VERSION** nastavena na hodnotu 6.
- Zachytávač AMS není podporován pro kanály AMQP nebo MQTT.

z/OS Advanced Message Security zachycení na kanálech zpráv

V systému z/OSposkytuje funkce odposlechu produktu Advanced Message Security (AMS) další volbu ochrany zásad zabezpečení (SPLPROT) pro kanály odesilatele, serveru, příjemce a žadatele, což vám umožňuje podporovat produkt AMS a komunikovat s obchodními partnery, kteří nepodporují produkt AMS.

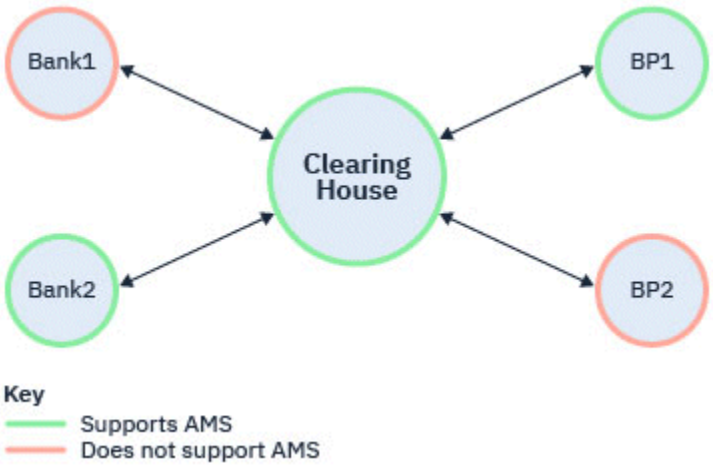
Vezmeme-li příklad clearingového střediska, které komunikuje s bankou, Obrázek 1 ukazuje, že bez AMS odposlechu musí obě strany systému podporovat AMS.



Obrázek 32. Použití AMS bez AMS odposlechu

Klíčovou výhodou volby AMS odposlechu je, že pokud váš podnik AMS nakonfiguroval a ne všichni vaši obchodní partneři podporují AMS, můžete odebrat ochranu před odchozími zprávami a chránit příchozí zprávy na kanálech těm obchodním partnerům, kteří nepodporují produkt AMS.

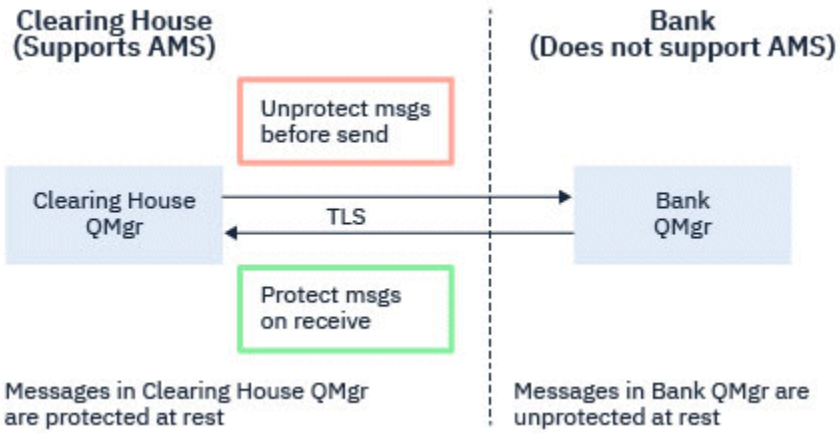
Pomocí příkladu clearingového střediska a bank je tento scénář zobrazen na Obrázku 2, kde existuje tok zpráv mezi clearingovým střediskem, bankami a obchodními partnery, kde některé instituce mají AMS, a jiné nikoli.



Obrázek 33. Někteří partneři podporují AMS a někteří ne

Kanály mají obvykle povolen protokol TLS.

Může se však jednat o případ, kdy některé banky a obchodní partneři nepodporují produkt AMSa existuje požadavek na možnost výměny zpráv mezi všemi bankami a obchodními partnery. Tento scénář je znázorněn na Obrázku 3



Obrázek 34. Tok zpráv mezi obchodními partnery

Související úlohy

Ukázkové konfigurace zachycování zpráv mezi servery

z/OS *Zachycení AMS na kanálech zpráv server-server*

Zachycení kanálu zpráv mezi servery poskytuje prostředky k řízení, zda by pro zprávy měly být použity vhodné zásady Advanced Message Security (AMS), když agenti kanálu zpráv typu odesilatel obdrží zprávy z přenosových front a agenti kanálu zpráv typu příjemce vkládají zprávy do cílových front.

To umožňuje povolit ochranu systému AMS ve správci front při komunikaci s použitím kanálů zpráv typu odesilatel, server, příjemce a žadatel typu server-server se správcem front, který nemá povolenou funkci AMS .

To znamená, že AMS chráněné zprávy v povolených správcích front systému AMS mohou být před odesláním nepovoleným správcům front systémuAMS nechráněné a nechráněné zprávy přijaté od nepovolených správců front systémuAMS mohou být chráněny příslušnými zásadami systému AMS v povolených správcích front systému AMS .

Konfigurace zachycení kanálu zpráv mezi servery

Zachycení kanálu zpráv mezi servery je konfigurováno s atributem SPLPROT na kanálech s typem kanálu odesilatel, server, příjemce nebo žadatel. Dostupné volby pro konfiguraci chování závisí na zadaném typu kanálu:

PASSTHRU
Projděte, beze změny, všechny zprávy odeslané nebo přijaté agentem MCA pro tento kanál.

Tato hodnota je platná pro kanály s typem kanálu (**CHLTYPE**) SDR, SVR, RCVR nebo RQSTR a jedná se o výchozí hodnotu.

REMOVE
Odeberte veškerou ochranu AMS před zprávami načtenými z přenosové fronty agentem MCA a odešlete zprávy partnerovi.

Když agent message obdrží zprávu z přenosové fronty a je pro přenosovou frontu definována zásada AMS, je uplatněna pro odebrání veškeré ochrany AMS ze zprávy před odesláním zprávy přes kanál. Není-li pro přenosovou frontu zásada AMS definována, je zpráva odeslána, jak je.

Tato hodnota je platná pouze pro kanály s typem SDR nebo SVR.

ASPOLICY
Na základě zásady definované pro cílovou frontu se uplatní ochrana AMS na příchozí zprávy před jejich vložením do cílové fronty.

Když agent MCA přijme příchozí zprávu a je pro cílovou frontu definována zásada AMS, uplatní se ochrana AMS na zprávu před jejím odesláním do cílové fronty. Není-li pro cílovou frontu definována zásada AMS, je zpráva vložena do cílové fronty, jak je.

Tato hodnota je platná pouze pro kanály s typem RCVR nebo RQSTR.

ID uživatele pro zachycení kanálu zpráv

Požadavky na ID uživatelů, která se používají s zachycením kanálu zpráv server-server, jsou stejné jako u existujících aplikací s povoleným produktem AMS . Pro spuštěný kanál získává odesílající agent kanálu zpráv z přenosové fronty a přijímající agent kanálu zpráv vkládá zprávy do cílových front. Pole MCAUSER (ID uživatele agenta kanálu zpráv), nastavené na serveru na kanály serveru, definuje ID uživatele, pod kterým agenti kanálu zpráv provádějí požadavky vložení a získání.

Při zachycení kanálu zpráv mezi servery jsou funkce AMS prováděny během požadavků na získání a vložení, stejně jako u jiných aplikací s povoleným produktem AMS . Proto mají ID uživatele agenta kanálu zpráv stejné požadavky jako ID uživatele aplikace AMS .

Atribut MCAUSER použitý k provedení operace vložení a získání je konfigurovatelný a závisí na tom, zda se jedná o odchozí nebo příchozí kanál. Podrobnosti o tom, jak vybrané ID uživatele provádí akce na agentu kanálu zpráv, viz MCAUSER . Jako takové je ID uživatele, pod kterým je spuštěn iniciátor kanálu, ID uživatele, které má být použito pro funkce AMS prováděné během zachycení kanálu zpráv mezi servery. Proto mají tato ID uživatelů stejné požadavky jako ID uživatelů aplikace AMS .

Ověření se provádí pomocí existujících pravidel pro kanál podrobný pro kanály s konfigurací PUTAUT. Další informace viz ID uživatelů používaná inicializátorem kanálu .

Poznámka: Zachycení kanálu zpráv mezi servery nebere v úvahu hodnotu atributu kanálu PUTAUT.

Velikost zprávy a MAXMSGL

Kvůli ochraně systému AMS bude velikost chráněných zpráv větší než velikost původní zprávy.

Chráněné zprávy jsou větší než nechráněné zprávy. Proto může být nutné změnit hodnotu atributu **MAXMSGL** ve frontách i v kanálech, aby se zohlednila velikost chráněných zpráv.

Související odkazy
Ukázkové konfigurace zachycování zpráv mezi servery

Ošetření chyb pro AMS

IBM MQ Advanced Message Security definuje frontu ošetření chyb pro správu zpráv, které obsahují chyby, nebo zprávy, které nemohou být nechráněné.

Vadné zprávy jsou řešeny jako výjimečné případy. Pokud přijatá zpráva nesplňuje požadavky na zabezpečení pro frontu, ve které se nachází, například pokud je zpráva podepsána, když by měla být zašifrována, nebo dešifrování nebo ověření podpisu selže, je zpráva odeslána do fronty ošetření chyb. Zpráva může být odeslána do fronty ošetření chyb z následujících důvodů:

- Neshoda kvality ochrany-neshoda kvality ochrany (QOP) existuje mezi přijatou zprávou a definicí QOP v zásadě zabezpečení.
- Chyba dešifrování-zprávu nelze dešifrovat.
- Chyba záhlaví PDMQ-k záhlaví zprávy Advanced Message Security (AMS) nelze přistupovat.
- Neshoda velikosti-délka zprávy po dešifrování je jiná, než se očekávalo.
- Neshoda síly šifrovacího algoritmu-šifrovací algoritmus zpráv je slabší, než je požadováno.
- Neznámá chyba-došlo k neočekávané chybě.

Produkt AMS používá systém SYSTEM.PROTECTION.ERROR.QUEUE jako svou frontu pro ošetření chyb. Všechny zprávy vložené systémem IBM MQ AMS do SYSTEM.PROTECTION.ERROR.QUEUE předchází záhlaví MQDLH.

Váš administrátor produktu IBM MQ může také definovat systém SYSTEM.PROTECTION.ERROR.QUEUE jako alias fronty odkazující na jinou frontu.

z/OS V systému IBM MQ 9.1.3, v systému IBM MQ for z/OS, pokud se používá zachycení agenta MCA (Message Channel Agent) serveru:

- Pokud z jednoho z výše uvedených důvodů produkt IBM MQ AMS přesune zprávy z přenosové fronty do fronty pro ošetření chyb, odesílatel MCA jednoduše pokračuje ve zpracování další dostupné zprávy v přenosové frontě.
- Obecně platí, že stávající pravidla kanálů platí pro:
  - Vkládání zpráv do fronty nedoručených zpráv a
  - Akce prováděné při vložení do fronty nedoručených zpráv by měly selhat.

Další informace o specifických scénářích viz “Nedoručené zprávy pro AMS on z/OS” na stránce 621 .

z/OS *Nedoručené zprávy pro AMS on z/OS*

Specifické scénáře související se zachycením agenta kanálu zpráv na serveru v systému IBM MQ for z/OS.

V systému IBM MQ 9.1.3, v systému IBM MQ for z/OS, pokud se používá zachycení agenta MCA (Message Channel Agent) serveru:

- Pokud po získání a nechránění zprávy odesilatel MCA z nějakého důvodu zprávu nedoručí, například proto, že je pro kanál příliš velká, pokud je atribut kanálu odesilatele USEDLQ nastaven na hodnotu YES, přesune odesílatel MCA zprávu do lokální fronty nedoručených zpráv (DLQ).

  Pokud je SYSTEM.DEAD.LETTER.QUEUE se používá jako lokální DLQ, zpráva je umístěna nechráněná.

  Poznámka: Produkt IBM MQ AMS nepodporuje ochranu zpráv vložených do systémových front.

  Pokud se jako lokální DLQ používá pojmenovaná DLQ, zpráva bude umístěna chráněná, pokud jste definovali zásadu IBM MQ AMS se stejným názvem jako pojmenovaná DLQ, a nechráněná, pokud jste nedefinovali vhodnou zásadu.
- Pokud zprávu z nějakého důvodu nelze vložit do lokální fronty DLQ, pak je-li parametr NPMSPEED kanálu nastaven na hodnotu NORMAL nebo je-li zpráva trvalou zprávou, je aktuální dávka zpráv vrácena zpět a kanál převeden do stavu RETRY. Jinak je zpráva vyřazena a odesílatel MCA pokračuje ve zpracování další zprávy v přenosové frontě.
- Vzhledem k tomu, že zásady zabezpečení nemají žádný vliv na systém SYSTEM.DEAD.LETTER.QUEUEnebo jiné fronty SYSTEM uvedené v seznamu “Ochrana systémové fronty

v produktu AMS” na stránce 694, pokud se jedná o SYSTEM.DEAD.LETTER.QUEUE se používá, zprávy vkládané do této fronty MCA jsou umístěny tak, jak jsou. To znamená, že pokud byly zprávy dříve chráněny, jsou umístěny chráněné; jinak jsou umístěny nechráněné.

Pokud byl atribut DEADQ správce front nastaven na název alternativní (nesystémové) fronty nedoručených zpráv a neexistuje zásada AMS se stejným názvem, jsou zprávy vkládané do této fronty MCA umístěny tak, jak jsou. To znamená, že pokud byly zprávy dříve chráněny, jsou umístěny chráněné; jinak jsou umístěny nechráněné.

Pokud byl atribut DEADQ správce front nastaven na název alternativní (nesystémové) fronty nedoručených zpráv a existuje zásada AMS se stejným názvem, jako má DLQ, použije se zásada k ochraně zpráv vložených do této fronty MCA. Pokud byla zpráva již dříve chráněna, není znovu chráněna; tím se zabrání dvojité ochraně. Pokud zásada AMS se stejným názvem neexistuje, jsou zprávy umístěny tak, jak jsou.

- Pokud existuje zásada pro DLQ s volbou tolerance v příkazu setmqspl nastavenou na hodnotu off, tj. '**-t** O', vložení do DLQ se nezdaří, pokud zpráva není AMS chráněná, a proto nemá záhlaví PDMQ. K tomu dochází v případě, že zpráva dorazí do příjemce bez záhlaví PDMQ. Jedná se o původní putter zprávy neměl zásadu pro cíl a příjemce nemá nastavenou hodnotu SPLPROT (ASPOLICY).
- Adaptéru MCA se nemusí podařit vložit zprávu do fronty DLQ, pokud zásada AMS definovaná pro frontu DLQ nepovoluje ID uživatele, pod kterým je spuštěn inicializátor kanálu, aby chránil zprávu.
- Přijímací kanály obvykle umisťují nedoručené zprávy do lokální fronty DLQ, zatímco odesílací kanály obecně umisťují zprávy, které nelze z nějakého důvodu zpracovat, například zprávy příliš velké pro frontu nebo chybné záhlaví MQXQH, atd. do lokální fronty DLQ.
- Obslužné rutiny DLQ se obecně dívají pouze na záhlaví DLQ (DLH), nikoli na samotný informační obsah zprávy. Takže skutečnost, že informační obsah zprávy může být chráněn, nebrání obslužným rutinám určit, proč byla zpráva umístěna do fronty DLQ.
- Není-li DLQ definováno, kanál:
  - Pokud nelze doručit trvalou zprávu, ukončí se nestandardně (a přejde do stavu opakování).
  - Zruší dočasnou nedoručenou zprávu a pokračuje v běhu.

Související pojmy

“Ošetření chyb pro AMS” na stránce 621
IBM MQ Advanced Message Security definuje frontu ošetření chyb pro správu zpráv, které obsahují chyby, nebo zprávy, které nemohou být nechráněné.

Uživatelské scénáře pro AMS

Seznamte se s možnými scénáři, abyste pochopili, jaké obchodní cíle můžete dosáhnout s produktem Advanced Message Security.

Windows *Stručná úvodní příručka pro AMS na platformách Windows*

Pomocí této příručky můžete rychle nakonfigurovat produkt Advanced Message Security (AMS) tak, aby poskytoval zabezpečení zpráv na platformách Windows . V době, kdy ji dokončíte, budete mít vytvořenou databázi klíčů pro ověření identit uživatelů a definovaných zásad podepisování a šifrování pro vašeho správce front.

Než začnete

V systému by měly být nainstalovány alespoň následující funkce:

- Server
- Development Toolkit (pro vzorové programy)
- Advanced Message Security (AMS)

Podrobnosti viz IBM MQ funkce pro Windows systémy .

Informace o použití příkazu **setmqenv** k inicializaci aktuálního prostředí tak, aby příslušné příkazy IBM MQ mohly být vyhledány a spuštěny operačním systémem, viz setmqenv (set IBM MQ environment).

1. Vytvoření správce front a fronty

Informace o této úloze

Všechny následující příklady používají frontu s názvem TEST.Q pro předávání zpráv mezi aplikacemi. Produkt Advanced Message Security používá zachytávače k podepisování a šifrování zpráv v okamžiku, kdy vstoupí do infrastruktury IBM MQ prostřednictvím standardního rozhraní IBM MQ . Základní nastavení se provádí v produktu IBM MQ a konfiguruje se v následujících krocích.

Pomocí produktu IBM MQ Explorer můžete vytvořit správce front QM_VERIFY_AMS a jeho lokální frontu s názvem TEST.Q pomocí všech výchozích nastavení průvodce nebo můžete použít příkazy nalezené v souboru `C:\Program Files\IBM\MQ\bin`. Nezapomeňte, že musíte být členem skupiny uživatelů `mqm` , abyste mohli spustit následující administrativní příkazy.

Postup

1. Vytvoření správce front

   ```
   crtmqm QM_VERIFY_AMS
   ```

2. Spustit správce front

   ```
   strmqm QM_VERIFY_AMS
   ```

3. Vytvořte frontu s názvem TEST.Q zadáním následujícího příkazu do adresáře **runmqsc** pro správce front QM_VERIFY_AMS .

   ```
   DEFINE QLOCAL(TEST.Q)
   ```

Výsledky

Pokud je procedura dokončena, příkaz zadaný do adresáře **runmqsc** zobrazí podrobnosti o TEST.Q:

```
DISPLAY Q(TEST.Q)
```

2. Vytvoření a autorizace uživatelů

Informace o této úloze

V tomto příkladu jsou uvedeni dva uživatelé: `alice`, odesilatel a bob, příjemce. Chcete-li používat frontu aplikací, těmto uživatelům musí být uděleno oprávnění k jejímu použití. Také pro úspěšné použití zásad ochrany, které budeme definovat tyto uživatele, musí být udělen přístup k některým systémovým frontám. Další informace o příkazu **setmqaut** viz **setmqaut**.

Postup

1. Vytvořte dva uživatele a ujistěte se, že HOMEPATH a HOMEDRIVE jsou nastaveny pro oba tyto uživatele.
2. Autorizovat uživatele pro připojení ke správci front a pro práci s frontou

   ```
   setmqaut -m QM_VERIFY_AMS -t qmgr -p alice -p bob +connect +inq
   ```

   ```
   setmqaut -m QM_VERIFY_AMS -n TEST.Q -t queue -p alice +put
   ```

```
setmqaut -m QM_VERIFY_AMS -n TEST.Q -t queue -p bob +get
```

3. Měli byste také umožnit oběma uživatelům procházet frontu systémových zásad a vkládat zprávy do fronty chyb.

```
setmqaut -m QM_VERIFY_AMS -t queue -n SYSTEM.PROTECTION.POLICY.QUEUE -p alice -p bob +browse
```

```
setmqaut -m QM_VERIFY_AMS -t queue -n SYSTEM.PROTECTION.ERROR.QUEUE -p alice -p bob +put
```

Upozornění: Produkt IBM MQ optimalizuje výkon ukládáním zásad do mezipaměti, abyste nemuseli procházet záznamy a hledat podrobnosti o zásadách v systému SYSTEM.PROTECTION.POLICY.QUEUE ve všech případech.

Produkt IBM MQ neukládá všechny dostupné zásady do mezipaměti. Pokud existuje vysoký počet zásad, produkt IBM MQ uloží do mezipaměti omezený počet zásad. Pokud má tedy správce front definován nízký počet zásad, není třeba systému SYSTEM.PROTECTION.POLICY.QUEUE.

Měli byste však udělit oprávnění k procházení této fronty v případě, že je definován vysoký počet zásad nebo pokud používáte staré klienty. Systém SYSTEM.PROTECTION.ERROR.QUEUE se používá k vložení chybových zpráv generovaných kódem AMS. Oprávnění vložení pro tuto frontu je kontrolováno pouze při pokusu o vložení chybové zprávy do fronty. Vaše oprávnění pro vložení do fronty není kontrolováno, když se pokusíte vložit nebo získat zprávu z chráněné fronty AMS.

Výsledky

Nyní jsou uživatelé vytvořeni a jsou jim udělena požadovaná oprávnění.

Jak pokračovat dále

Chcete-li ověřit, zda byly kroky provedeny správně, použijte ukázky `amqsput` a `amqsget` , jak je popsáno v části “7. Testování nastavení” na stránce 627.

3. Vytvoření databáze klíčů a certifikátů

Informace o této úloze

Zachytávač vyžaduje veřejný klíč odesílajících uživatelů k zašifrování zprávy. Proto musí být vytvořena databáze klíčů identit uživatelů mapovaných na veřejné a soukromé klíče. V reálném systému, kde jsou uživatelé a aplikace rozptýleny na několika počítačích, by měl každý uživatel své vlastní soukromé úložiště klíčů. Podobně v této příručce vytváříme databáze klíčů pro `alice` a bob a sdílíme mezi nimi uživatelské certifikáty.

Poznámka: V této příručce používáme ukázkové aplikace napsané v jazyce C, které se připojují pomocí lokálních vazeb. Pokud plánujete používat aplikace Java používající vazby klienta, musíte vytvořit úložiště klíčů JKS a certifikáty pomocí příkazu **`keytool`** , který je součástí prostředí JRE (další podrobnosti viz “Stručná úvodní příručka pro klienty AMS with Java” na stránce 645). Pro všechny ostatní jazyky a pro aplikace Java používající lokální vazby jsou kroky v této příručce správné.

Postup

1. Použijte grafické rozhraní produktu IBM Key Management (`strmqikm.exe`) k vytvoření nové databáze klíčů pro uživatele `alice`.

```
Type:       CMS
Filename:   alicekey.kdb
Location:   C:/Documents and Settings/alice/AMS
```

Poznámka:

- K zabezpečení databáze je vhodné použít silné heslo.
- Ujistěte se, že je zaškrtnuto políčko **Ukrýt heslo do souboru** .

2. Změňte zobrazení obsahu databáze klíčů na **Osobní certifikáty**.
3. Vyberte volbu **Nový podepsaný sebou samým** ; V tomto scénáři se používají certifikáty podepsané sebou samým.
4. Vytvořte certifikát identifikující uživatele `alice` pro použití v šifrování pomocí těchto polí:

```
Key label: Alice_Cert
Common Name: alice
Organisation: IBM
Country: GB
```

Poznámka:

- Pro účely této příručky používáme certifikát podepsaný svým držitelem, který lze vytvořit bez použití certifikační autority. U produkčních systémů se doporučuje nepoužívat certifikáty podepsané svým držitelem, ale spoléhat se na certifikáty podepsané certifikační autoritou.
- Parametr **`Key label`** určuje název certifikátu, který zachytávače vyhledají, aby obdržely nezbytné informace.
- Parametr **`Common Name`** a volitelné parametry uvádí podrobnosti o **rozlišujícím názvu** (DN), které musí být pro každého uživatele jedinečné.

5. Opakujte krok 1-4 pro uživatele bob

Výsledky

Oba uživatelé `alice` a bob mají nyní certifikát podepsaný svým držitelem.

4. Vytvoření souboru keystore.conf

Informace o této úloze

Musíte odvést zachytávače Advanced Message Security do adresáře, kde jsou umístěny databáze klíčů a certifikáty. To se provádí prostřednictvím souboru `keystore.conf` , který uchovává tyto informace ve formátu prostého textu. Každý uživatel musí mít ve složce `.mqs` samostatný soubor `keystore.conf` . Tento krok musí být proveden pro `alice` i bob.

Obsah souboru `keystore.conf` musí být ve tvaru:

```
cms.keystore = dir/keystore_file
cms.certificate = certificate_label
```

Příklad

Pro tento scénář bude obsah souboru `keystore.conf` následující:

```
cms.keystore = C:/Documents and Settings/alice/AMS/alicekey
cms.certificate = Alice_Cert
```

Poznámka:

- Cesta k souboru úložiště klíčů musí být poskytnuta bez přípony souboru.
- Popisek certifikátu může obsahovat mezery, tedy "Alice_Cert" a "Alice_Cert" (s mezerou na konci) jsou například rozpoznány jako popisky dvou různých certifikátů. Chcete-li se však vyhnout nejasnostem, je lepší nepoužívat v názvu popisku mezery.

- Existují následující formáty úložiště klíčů: CMS (Cryptographic Message Syntax), JKS (Java keystore) a JCEKS (Java Cryptographic Extension Keystore). Další informace jsou uvedeny v tématu “Struktura konfiguračního souboru úložiště klíčů (keystore.conf) pro AMS” na stránce 658.
- *%HOMEDRIVE%\%HOMEPATH%*\.mqs\keystore.conf (např. C:\Documents a Settings\alice\.mqs\keystore.conf) je výchozí umístění, kde produkt Advanced Message Security hledá soubor keystore.conf . Chcete-li získat informace o tom, jak použít jiné než výchozí umístění pro keystore.conf, prohlédněte si téma “Použití úložišť klíčů a certifikátů s produktem AMS” na stránce 657.
- Chcete-li vytvořit adresář .mqs , musíte použít příkazový řádek.

5. Sdílení certifikátů

Informace o této úloze

Sdílejte certifikáty mezi těmito dvěma databázemi klíčů, aby každý uživatel mohl úspěšně identifikovat druhého. To se provádí extrahováním veřejného certifikátu každého uživatele do souboru, který je poté přidán do databáze klíčů jiného uživatele.

Poznámka: Dávejte pozor, abyste použili volbu *extract* , a ne volbu *export* . *Extrahovat* získá veřejný klíč uživatele, zatímco *export* získá veřejný i soukromý klíč. Chybné použití *exportu* by zcela ohrozilo vaši aplikaci předáním jejího soukromého klíče.

Postup

1. Extrahujte certifikát identifikující alice do externího souboru:

```
runmqakm -cert -extract -db "C:/Documents and Settings/alice/AMS/alicekey.kdb" -pw passw0rd
-label Alice_Cert -target alice_public.arm
```

2. Přidejte certifikát do úložiště klíčů bob's :

```
runmqakm -cert -add -db "C:/Documents and Settings/bob/AMS/bobkey.kdb" -pw passw0rd -label
Alice_Cert -file alice_public.arm
```

3. Opakujte kroky pro bob:

```
runmqakm -cert -extract -db "C:/Documents and Settings/bob/AMS/bobkey.kdb" -pw passw0rd
-label Bob_Cert -target bob_public.arm
```

```
runmqakm -cert -add -db "C:/Documents and Settings/alice/AMS/alicekey.kdb" -pw passw0rd
-label Bob_Cert -file bob_public.arm
```

Výsledky

Dva uživatelé alice a bob se nyní mohou úspěšně identifikovat, zda vytvořili a sdíleli certifikáty podepsané sebou samým.

Jak pokračovat dále

Ověřte, že je certifikát v úložišti klíčů, buď jeho procházením pomocí grafického rozhraní, nebo spuštěním následujících příkazů, které vytisknou jeho podrobnosti:

```
runmqakm -cert -details -db "C:/Documents and Settings/bob/AMS/bobkey.kdb" -pw passw0rd -label
Alice_Cert
```

```
runmqakm -cert -details -db "C:/Documents and Settings/alice/AMS/alicekey.kdb" -pw passw0rd
-label Bob_Cert
```

6. Definování zásady fronty

Informace o této úloze

S vytvořeným správcem front a zachytávači připravenými k zachycení zpráv a přístupu k šifrovacím klíčům můžeme začít definovat zásady ochrany v systému QM_VERIFY_AMS pomocí příkazu `setmqspl` . Další informace o tomto příkazu viz setmqspl . Každý název zásady musí být stejný jako název fronty, na kterou se má použít.

Příklad

Toto je příklad zásady definované pro frontu `TEST.Q` . V tomto příkladu jsou zprávy podepsány algoritmem Deprecated SHA1 a zašifrovány algoritmem AES256 . `alice` je jediným platným odesilatelem a bob je jediným příjemcem zpráv v této frontě:

```
setmqspl -m QM_VERIFY_AMS -p TEST.Q -s SHA1 -a "CN=alice,O=IBM,C=GB" -e AES256 -r
"CN=bob,O=IBM,C=GB"
```

Poznámka: DN se přesně shodují s těmi, která jsou uvedena v příslušném certifikátu uživatele z databáze klíčů.

Jak pokračovat dále

Chcete-li ověřit zásadu, kterou jste definovali, zadejte následující příkaz:

```
dspmqspl -m QM_VERIFY_AMS
```

Chcete-li vytisknout podrobnosti zásady jako sadu příkazů `setmqspl` , použijte příznak `-export` . To umožňuje ukládání již definovaných zásad:

```
dspmqspl -m QM_VERIFY_AMS -export >restore_my_policies.bat
```

7. Testování nastavení

Informace o této úloze

Spuštěním různých programů pod různými uživateli můžete ověřit, zda byla aplikace správně nakonfigurována.

Postup

1. Přepnout uživatele, aby se spustil jako uživatel `alice`

   Klepněte pravým tlačítkem myši na `cmd.exe` a vyberte volbu **Spustit jako ...**. Po zobrazení výzvy se přihlaste jako uživatel `alice`.
2. Jak uživatel `alice` vložil zprávu pomocí ukázkové aplikace:

   ```
   amqsput TEST.Q QM_VERIFY_AMS
   ```
3. Zadejte text zprávy a stiskněte klávesu Enter.
4. Přepnout uživatele, aby se spustil jako uživatel bob

   Otevřete další okno klepnutím pravým tlačítkem myši na soubor `cmd.exe` a výběrem volby **Spustit jako ...**. Po zobrazení výzvy se přihlaste jako uživatel bob.
5. Jak uživatel bob získá zprávu pomocí ukázkové aplikace:

   ```
   amqsget TEST.Q QM_VERIFY_AMS
   ```

Výsledky

Pokud byla aplikace správně nakonfigurována pro oba uživatele, zobrazí se zpráva uživatele `alice` , když produkt bob spustí získávanou aplikaci.

8. Testování šifrování

Informace o této úloze

Chcete-li ověřit, že k šifrování dochází podle očekávání, vytvořte alias frontu, která odkazuje na původní frontu `TEST.Q`. Tato fronta aliasů nebude mít žádnou zásadu zabezpečení, takže žádný uživatel nebude mít informace k dešifrování zprávy, a proto budou zobrazena šifrovaná data.

Postup

1. Pomocí příkazu **runmqsc** pro správce front QM_VERIFY_AMS vytvořte alias frontu.

```
DEFINE QALIAS(TEST.ALIAS) TARGET(TEST.Q)
```

2. Udělit přístup bob pro procházení z alias fronty

```
setmqaut -m QM_VERIFY_AMS -n TEST.ALIAS -t queue -p bob +browse
```

3. Jako uživatel `alice`vložte další zprávu pomocí ukázkové aplikace stejně jako dříve:

```
amqsput TEST.Q QM_VERIFY_AMS
```

4. Jako uživatel bobnyní procházejte zprávu pomocí ukázkové aplikace prostřednictvím fronty aliasů:

```
amqsbcg TEST.ALIAS QM_VERIFY_AMS
```

5. Jako uživatel bobzískejte zprávu pomocí ukázkové aplikace z lokální fronty:

```
amqsget TEST.Q QM_VERIFY_AMS
```

Výsledky

Výstup z aplikace `amqsbcg` zobrazuje šifrovaná data, která jsou ve frontě, prokazující, že zpráva byla šifrována.

Linux AIX *Stručná úvodní příručka pro AMS on AIX and Linux*

Pomocí této příručky můžete rychle konfigurovat produkt Advanced Message Security tak, aby poskytoval zabezpečení zpráv v systému AIX and Linux. V době, kdy jej dokončíte, budete mít vytvořenou databázi klíčů pro ověření identit uživatelů a definované zásady podepisování a šifrování pro vašeho správce front.

Než začnete

V systému by měly být nainstalovány alespoň následující komponenty:

- Běhové prostředí
- Server
- Ukázkové programy.
- IBM Global Security Kit (GSKit)
- Advanced Message Security

Názvy komponent na každé specifické platformě naleznete v následujících tématech:

- Linux IBM MQ komponenty pro Linux systémy

- AIX IBM MQ komponenty pro AIX systémy

1. Vytvoření správce front a fronty

Informace o této úloze

Všechny následující příklady používají frontu s názvem TEST.Q pro předávání zpráv mezi aplikacemi. Produkt Advanced Message Security používá zachytávače k podepisování a šifrování zpráv v okamžiku, kdy vstoupí do infrastruktury IBM MQ prostřednictvím standardního rozhraní IBM MQ . Základní nastavení se provádí v produktu IBM MQ a konfiguruje se v následujících krocích.

Pomocí produktu IBM MQ Explorer můžete vytvořit správce front QM_VERIFY_AMS a jeho lokální frontu s názvem TEST.Q pomocí všech výchozích nastavení průvodce nebo můžete použít příkazy nalezené v souboru *MQ_INSTALLATION_PATH*/bin. Nezapomeňte, že musíte být členem skupiny uživatelů mqm , abyste mohli spustit následující administrativní příkazy.

Postup

1. Vytvoření správce front

```
crtmqm QM_VERIFY_AMS
```

2. Spustit správce front

```
strmqm QM_VERIFY_AMS
```

3. Vytvořte frontu s názvem TEST.Q zadáním následujícího příkazu do adresáře **runmqsc** pro správce front QM_VERIFY_AMS .

```
DEFINE QLOCAL(TEST.Q)
```

Výsledky

Pokud byla procedura úspěšně dokončena, následující příkaz zadaný do adresáře **runmqsc** zobrazí podrobnosti o souboru TEST.Q:

```
DISPLAY Q(TEST.Q)
```

2. Vytvoření a autorizace uživatelů

Informace o této úloze

V tomto příkladu jsou uvedeni dva uživatelé: alice, odesilatel a bob, příjemce. Chcete-li používat frontu aplikací, těmto uživatelům musí být uděleno oprávnění k jejímu použití. Také pro úspěšné použití zásad ochrany, které budeme definovat tyto uživatele, musí být udělen přístup k některým systémovým frontám. Další informace o příkazu **setmqaut** viz **setmqaut**.

Postup

1. Vytvořit dva uživatele

```
useradd alice
```

```
useradd bob
```

2. Autorizovat uživatele pro připojení ke správci front a pro práci s frontou

```
setmqaut -m QM_VERIFY_AMS -t qmgr -p alice -p bob +connect +inq
```

```
setmqaut -m QM_VERIFY_AMS -n TEST.Q -t queue -p alice +put
```

```
setmqaut -m QM_VERIFY_AMS -n TEST.Q -t queue -p bob +get
```

3. Měli byste také umožnit oběma uživatelům procházet frontu systémových zásad a vkládat zprávy do fronty chyb.

```
setmqaut -m QM_VERIFY_AMS -t queue -n SYSTEM.PROTECTION.POLICY.QUEUE -p alice -p bob +browse
```

```
setmqaut -m QM_VERIFY_AMS -t queue -n SYSTEM.PROTECTION.ERROR.QUEUE -p alice -p bob +put
```

Upozornění: Produkt IBM MQ optimalizuje výkon ukládáním zásad do mezipaměti, abyste nemuseli procházet záznamy a hledat podrobnosti o zásadách v systému SYSTEM.PROTECTION.POLICY.QUEUE ve všech případech.

Produkt IBM MQ neukládá všechny dostupné zásady do mezipaměti. Pokud existuje vysoký počet zásad, produkt IBM MQ uloží do mezipaměti omezený počet zásad. Pokud má tedy správce front definován nízký počet zásad, není třeba systému SYSTEM.PROTECTION.POLICY.QUEUE.

Měli byste však udělit oprávnění k procházení této fronty v případě, že je definován vysoký počet zásad nebo pokud používáte staré klienty. Systém SYSTEM.PROTECTION.ERROR.QUEUE se používá k vložení chybových zpráv generovaných kódem AMS. Oprávnění vložení pro tuto frontu je kontrolováno pouze při pokusu o vložení chybové zprávy do fronty. Vaše oprávnění pro vložení do fronty není kontrolováno, když se pokusíte vložit nebo získat zprávu z chráněné fronty AMS.

Výsledky

Nyní jsou vytvořeny skupiny uživatelů a jsou jim udělena požadovaná oprávnění. Tímto způsobem budou mít uživatelé přiřazení k těmto skupinám také oprávnění pro připojení ke správci front a pro vložení a získání z fronty.

Jak pokračovat dále

Chcete-li ověřit, zda byly kroky provedeny správně, použijte ukázky `amqsput` a `amqsget` , jak je popsáno v části “8. Testování šifrování” na stránce 634.

3. Vytvoření databáze klíčů a certifikátů

Informace o této úloze

K zašifrování zprávy zachytávač vyžaduje soukromý klíč odesílajícího uživatele a veřejný klíč (y) příjemce (ů). Proto musí být vytvořena databáze klíčů identit uživatelů mapovaných na veřejné a soukromé klíče. V reálném systému, kde jsou uživatelé a aplikace rozptýleny na několika počítačích, by měl každý uživatel své vlastní soukromé úložiště klíčů. Podobně v této příručce vytváříme databáze klíčů pro `alice` a bob a sdílíme mezi nimi uživatelské certifikáty.

Poznámka: V této příručce používáme ukázkové aplikace napsané v jazyce C, které se připojují pomocí lokálních vazeb. Pokud plánujete používat aplikace Java používající vazby klienta, musíte vytvořit úložiště klíčů JKS a certifikáty pomocí příkazu **keytool** , který je součástí prostředí JRE (další podrobnosti viz “Stručná úvodní příručka pro klienty AMS with Java” na stránce 645). Pro všechny ostatní jazyky a pro aplikace Java používající lokální vazby jsou kroky v této příručce správné.

Postup

1. Vytvořit novou databázi klíčů pro uživatele `alice`

```
mkdir /home/alice/.mqs -p
```

```
runmqakm -keydb -create -db /home/alice/.mqs/alicekey.kdb -pw passw0rd -stash
```

Poznámka:

- K zabezpečení databáze je vhodné použít silné heslo.
- Parametr **`stash`** ukládá heslo do souboru `key.sth` , který zachytávače mohou použít k otevření databáze.

2. Ujistěte se, že je databáze klíčů čitelná

```
chmod +r /home/alice/.mqs/alicekey.kdb
```

3. Vytvořte certifikát identifikující uživatele `alice` pro použití v šifrování

```
runmqakm -cert -create -db /home/alice/.mqs/alicekey.kdb -pw passw0rd -label Alice_Cert -dn
"cn=alice,O=IBM,c=GB" -default_cert yes
```

Poznámka:

- Pro účely této příručky používáme certifikát podepsaný svým držitelem, který lze vytvořit bez použití certifikační autority. U produkčních systémů se doporučuje nepoužívat certifikáty podepsané sebou samým, ale spoléhat se na certifikáty podepsané certifikační autoritou.
- Parametr **`label`** určuje název certifikátu, který zachytávače vyhledají, aby obdržely nezbytné informace.
- Parametr **DN** uvádí podrobnosti o **rozlišujícím názvu** (DN), který musí být pro každého uživatele jedinečný.

4. Nyní jsme vytvořili databázi klíčů, měli bychom nastavit její vlastnictví a zajistit, aby byla nečitelná pro všechny ostatní uživatele.

```
chown alice /home/alice/.mqs/alicekey.kdb /home/alice/.mqs/alicekey.sth
```

```
chmod 600 /home/alice/.mqs/alicekey.kdb /home/alice/.mqs/alicekey.sth
```

5. Opakujte krok 1-4 pro uživatele bob

Výsledky

Oba uživatelé `alice` a bob mají nyní certifikát podepsaný svým držitelem.

4. Vytvoření souboru keystore.conf

Informace o této úloze

Musíte odvést zachytávače Advanced Message Security do adresáře, kde jsou umístěny databáze klíčů a certifikáty. To se provádí prostřednictvím souboru `keystore.conf` , který uchovává tyto informace ve formátu prostého textu. Každý uživatel musí mít ve složce `.mqs` samostatný soubor `keystore.conf` . Tento krok musí být proveden pro `alice` i bob.

Obsah souboru `keystore.conf` musí být ve tvaru:

```
cms.keystore = dir/keystore_file
```

```
cms.certificate = certificate_label
```

Příklad

Pro tento scénář bude obsah souboru `keystore.conf` následující:

```
cms.keystore = /home/alice/.mqs/alicekey
cms.certificate = Alice_Cert
```

Poznámka:

- Cesta k souboru úložiště klíčů musí být poskytnuta bez přípony souboru.
- Existují následující formáty úložiště klíčů: CMS (Cryptographic Message Syntax), JKS (Java keystore) a JCEKS (Java Cryptographic Extension Keystore). Další informace jsou uvedeny v tématu “Struktura konfiguračního souboru úložiště klíčů (keystore.conf) pro AMS” na stránce 658.
- `HOME/.mqs/keystore.conf` je výchozí umístění, kde produkt Advanced Message Security hledá soubor `keystore.conf` . Chcete-li získat informace o tom, jak použít jiné než výchozí umístění pro `keystore.conf`, prohlédněte si téma “Použití úložišť klíčů a certifikátů s produktem AMS” na stránce 657.

5. Sdílení certifikátů

Informace o této úloze

Sdílejte certifikáty mezi dvěma databázemi klíčů, aby každý uživatel mohl úspěšně identifikovat druhého. To se provádí extrahováním veřejného certifikátu každého uživatele do souboru, který je poté přidán do databáze klíčů jiného uživatele.

Poznámka: Dávejte pozor, abyste použili volbu *extract* , a ne volbu *export* . *Extrahovat* získá veřejný klíč uživatele, zatímco *export* získá veřejný i soukromý klíč. Chybné použití *exportu* by zcela ohrozilo vaši aplikaci předáním jejího soukromého klíče.

Postup

1. Extrahujte certifikát identifikující `alice` do externího souboru:

   ```
   runmqakm -cert -extract -db /home/alice/.mqs/alicekey.kdb -pw passw0rd -label Alice_Cert
   -target alice_public.arm
   ```

2. Přidejte certifikát do úložiště klíčů `bob's` :

   ```
   runmqakm -cert -add -db /home/bob/.mqs/bobkey.kdb -pw passw0rd -label Alice_Cert -file
   alice_public.arm
   ```

3. Zopakujte krok pro bob:

   ```
   runmqakm -cert -extract -db /home/bob/.mqs/bobkey.kdb -pw passw0rd -label Bob_Cert -target
   bob_public.arm
   ```

4. Přidejte certifikát pro bob do úložiště klíčů `alice's` :

   ```
   runmqakm -cert -add -db /home/alice/.mqs/alicekey.kdb -pw passw0rd -label Bob_Cert -file
   bob_public.arm
   ```

Výsledky

Dva uživatelé `alice` a bob se nyní mohou úspěšně identifikovat, zda vytvořili a sdíleli certifikáty podepsané sebou samým.

Jak pokračovat dále

Ověřte, že je certifikát v úložišti klíčů, spuštěním následujících příkazů, které vytisknou jeho podrobnosti:

```
runmqakm -cert -details -db /home/bob/.mqs/bobkey.kdb -pw passw0rd -label Alice_Cert
```

```
runmqakm -cert -details -db /home/alice/.mqs/alicekey.kdb -pw passw0rd -label Bob_Cert
```

6. Definování zásady fronty

Informace o této úloze

S vytvořeným správcem front a zachytávači připravenými k zachycení zpráv a přístupu k šifrovacím klíčům můžeme začít definovat zásady ochrany v systému QM_VERIFY_AMS pomocí příkazu `setmqspl` . Další informace o tomto příkazu viz setmqspl . Každý název zásady musí být stejný jako název fronty, na kterou se má použít.

Příklad

Toto je příklad zásady definované pro frontu `TEST.Q` . V tomto příkladu jsou zprávy podepsány uživatelem `alice` pomocí algoritmu Deprecated SHA1 a zašifrovány pomocí 256bitového algoritmu AES . `alice` je jediným platným odesilatelem a bob je jediným příjemcem zpráv v této frontě:

```
setmqspl -m QM_VERIFY_AMS -p TEST.Q -s SHA1 -a "CN=alice,O=IBM,C=GB" -e AES256 -r
"CN=bob,O=IBM,C=GB"
```

Poznámka: Rozlišující názvy se přesně shodují s těmi, které jsou uvedeny v příslušném certifikátu uživatele z databáze klíčů.

Jak pokračovat dále

Chcete-li ověřit zásadu, kterou jste definovali, zadejte následující příkaz:

```
dspmqspl -m QM_VERIFY_AMS
```

Chcete-li vytisknout podrobnosti zásady jako sadu příkazů `setmqspl` , použijte příznak `-export` . To umožňuje ukládání již definovaných zásad:

```
dspmqspl -m QM_VERIFY_AMS -export >restore_my_policies.bat
```

7. Testování nastavení

Informace o této úloze

Spuštěním různých programů pod různými uživateli můžete ověřit, zda byla aplikace správně nakonfigurována.

Postup

1. Přejděte do adresáře obsahujícího ukázky. Pokud je produkt MQ instalován v jiném než výchozím umístění, může se jednat o jiné místo.

   ```
   cd /opt/mqm/samp/bin
   ```

2. Přepnout uživatele, aby se spustil jako uživatel `alice`

   ```
   su alice
   ```

3. Jako uživatel `alice`vložte zprávu pomocí ukázkové aplikace:

```
./amqsput TEST.Q QM_VERIFY_AMS
```

4. Zadejte text zprávy a stiskněte klávesu Enter.
5. Zastavit spuštění jako uživatel `alice`

```
exit
```

6. Přepnout uživatele, aby se spustil jako uživatel bob

```
su bob
```

7. Jako uživatel bobzískejte zprávu pomocí ukázkové aplikace:

```
./amqsget TEST.Q QM_VERIFY_AMS
```

Výsledky

Pokud byla aplikace správně nakonfigurována pro oba uživatele, zobrazí se zpráva uživatele `alice` , když produkt bob spustí získávanou aplikaci.

8. Testování šifrování

Informace o této úloze

Chcete-li ověřit, že šifrování probíhá podle očekávání, vytvořte alias frontu, která odkazuje na původní frontu `TEST.Q`. Tato fronta aliasů nebude mít žádnou zásadu zabezpečení, takže žádný uživatel nebude mít informace k dešifrování zprávy, a proto budou zobrazena šifrovaná data.

Postup

1. Pomocí příkazu **`runmqsc`** pro správce front QM_VERIFY_AMS vytvořte alias frontu.

```
DEFINE QALIAS(TEST.ALIAS) TARGET(TEST.Q)
```

2. Udělit přístup bob pro procházení z alias fronty

```
setmqaut -m QM_VERIFY_AMS -n TEST.ALIAS -t queue -p bob +browse
```

3. Jako uživatel `alice`vložte další zprávu pomocí ukázkové aplikace stejně jako dříve:

```
./amqsput TEST.Q QM_VERIFY_AMS
```

4. Jako uživatel bobnyní procházejte zprávu pomocí ukázkové aplikace prostřednictvím fronty aliasů:

```
./amqsbcg TEST.ALIAS QM_VERIFY_AMS
```

5. Jako uživatel bobzískejte zprávu pomocí ukázkové aplikace z lokální fronty:

```
./amqsget TEST.Q QM_VERIFY_AMS
```

Výsledky

Výstup z aplikace `amqsbcg` zobrazí šifrovaná data, která jsou ve frontě, prokazující, že zpráva byla šifrována.

z/OS *Příklad AMS konfigurací na systému z/OS*

V této části jsou uvedeny příklady konfigurací zásad a certifikátů pro Advanced Message Security scénáře řazení do front v systému z/OS.

Podrobné informace o konfiguraci produktu Advanced Message Securitynaleznete v tématu Konfigurace produktu Advanced Message Security for z/OS .

Příklady zahrnují požadované zásady Advanced Message Security a digitální certifikáty, které musí existovat vzhledem k uživatelům a klíčům. Příklady předpokládají, že uživatelé zapojení do scénářů byli nastaveni podle pokynů uvedených v části Udělit uživatelům oprávnění k prostředkům pro produkt Advanced Message Security.

Dále, od IBM MQ 9.1.3 dále, viz příklady zachycování kanálů zpráv server-server.

z/OS *Lokální řazení zpráv chráněných integritou do fronty pro AMS on z/OS*

Tento příklad uvádí podrobnosti o zásadách Advanced Message Security a certifikátech potřebných k odeslání a načtení zpráv chráněných integritou do fronty a z fronty, lokální pro vkládající a načítající aplikace.

Příkladem správce front a fronty jsou:

```
BNK6        - Queue manager
FIN.XFER.Q7 - Local queue
```

Používají se tito uživatelé:

```
WMQBNK6  - AMS task user
TELLER5  - Sending user
FINADM2  - Recipient user
```

Vytvořit uživatelské certifikáty

V tomto příkladu je potřeba pouze jeden uživatelský certifikát. Toto je odesílající certifikát uživatele, který je potřebný k podepsání zpráv chráněných integritou. Odesílající uživatel je 'TELLER5'.

Požaduje se také certifikát certifikační autority (CA). Certifikát CA je certifikát autority, která vydala certifikát uživatele. Může se jednat o řetězec certifikátů. Pokud ano, všechny certifikáty v řetězci jsou vyžadovány v svazku klíčů uživatele úlohy Advanced Message Security , v tomto případě uživatele WMQBNK6.

Certifikát CA lze vytvořit pomocí příkazu RACF RACDCERT. Tento certifikát se používá k vydávání uživatelských certifikátů. Příklad:

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('BCOCA') O('BCO') C('US'))
KEYUSAGE(CERTSIGN) WITHLABEL('BCOCA')
```

Tento příkaz RACDCERT vytvoří certifikát CA, který pak může být použit k vydání uživatelského certifikátu pro uživatele 'TELLER5'. Příklad:

```
RACDCERT ID(TELLER5) GENCERT SUBJECTSDN(CN('Teller5') O('BCO') C('US'))
WITHLABEL('Teller5') SIGNWITH(CERTAUTH LABEL('BCOCA'))KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)
```

Vaše instalace bude mít postupy pro výběr nebo vytvoření certifikátu CA, stejně jako postupy pro vydávání certifikátů a jejich distribuci do příslušných systémů.

Při exportu a importu těchto certifikátů produkt Advanced Message Security vyžaduje:

- Certifikát CA (řetěz).
- Uživatelský certifikát a jeho soukromý klíč.

Pokud používáte produkt RACF, příkaz RACDCERT EXPORT lze použít k exportu certifikátů do datové sady a příkaz RACDCERT ADD lze použít k importu certifikátů z datové sady. Další informace o těchto a dalších příkazech RACDCERT naleznete v příručce *z/OS: Security Server RACF Command Language Reference*.

V tomto případě jsou vyžadovány certifikáty v systému z/OS , na kterém je spuštěn správce front BNK6.

Když byly certifikáty importovány do systému z/OS , na kterém běží BNK6, uživatelský certifikát vyžaduje atribut TRUST. K přidání atributu TRUST do certifikátu lze použít příkaz ALTER RACDCERT. Příklad:

```
RACDCERT ID(TELLER5) ALTER (LABEL('Teller5')) TRUST
```

V tomto příkladu není pro uživatele příjemce vyžadován žádný certifikát.

Připojit certifikáty k příslušným kroužkům klíčů

Když byly požadované certifikáty vytvořeny nebo importovány a nastaveny jako důvěryhodné, musí být připojeny k příslušným kroužkům klíčů uživatele na systému z/OS , na kterém běží BNK6. Chcete-li vytvořit svazky klíčů, použijte příkazy RACDCERT ADDRING:

```
RACDCERT ID(WMQBNK6) ADDRING(drq.ams.keyring)
```

```
RACDCERT ID(TELLER5) ADDRING(drq.ams.keyring)
```

Tím se vytvoří svazek klíčů pro uživatele úlohy Advanced Message Security WMQBNK6a svazek klíčů pro odesílajícího uživatele 'TELLER5'. Všimněte si, že název svazku klíčů drq.ams.keyring je povinný a název rozlišuje velikost písmen.

Po vytvoření klíčových kroužků lze příslušné certifikáty připojit:

```
RACDCERT ID(WMQBNK6) CONNECT(CERTAUTH LABEL('BCOCA')
RING(drq.ams.keyring))
```

```
RACDCERT ID(TELLER5) CONNECT(ID(TELLER5) LABEL('Teller5')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
```

Odesílající uživatelský certifikát musí být připojen jako DEFAULT. Pokud má odesílající uživatel ve svém drq.ams.keyringvíce než jeden certifikát, použije se pro účely podepisování výchozí certifikát.

Vytvoření a úprava certifikátů není produktem Advanced Message Security rozpoznána, dokud není správce front zastaven a restartován, nebo dokud není příkaz z/OS **MODIFY** použit k aktualizaci konfigurace certifikátu Advanced Message Security . Příklad:

```
F BNK6AMSM,REFRESH KEYRING
```

Vytvořit zásadu Advanced Message Security

V tomto příkladu jsou zprávy chráněné integritou vloženy do fronty FIN.XFER.Q7 aplikací spuštěnou jako uživatel 'TELLER5' a načtenou ze stejné fronty aplikací spuštěnou jako uživatel 'FINADM2', takže je požadována pouze jedna zásada Advanced Message Security .

Zásady systému Advanced Message Security jsou vytvořeny pomocí obslužného programu CSQ0UTIL , který je dokumentován v tématu Obslužný program zásad zabezpečení zpráv (CSQ0UTIL).

Pomocí obslužného programu CSQ0UTIL spusťte následující příkaz:

```
setmqspl -m BNK6 -p FIN.XFER.Q7 -s MD5 -a CN=Teller5,O=BCO,C=US
```

V této zásadě je správce front identifikován jako BNK6. Název zásady a přidružená fronta jsou FIN.XFER.Q7. Algoritmus použitý ke generování podpisu odesílatele je MD5a rozlišující název (DN) odesílajícího uživatele je 'CN=Teller5,O=BCO,C=US'.

Po definování zásady buď restartujte správce front BNK6 , nebo pomocí příkazu z/OS **MODIFY** aktualizujte konfiguraci zásady Advanced Message Security . Příklad:

```
F BNK6AMSM,REFRESH POLICY
```

z/OS *Lokální řazení zpráv chráněných soukromím do fronty pro AMS on z/OS*

Tento příklad podrobně popisuje zásady a certifikáty Advanced Message Security potřebné k odesílání a načítání zpráv chráněných ochranou soukromí do fronty a z fronty, lokální pro vkládající a načítající aplikace. Zprávy chráněné ochranou soukromí jsou podepsané i šifrované.

Příklad správce front a lokální fronta jsou následující:

```
BNK6        - Queue manager
FIN.XFER.Q8 - Local queue
```

Používají se tito uživatelé:

```
WMQBNK6  - AMS task user
TELLER5  - Sending user
FINADM2  - Recipient user
```

Postup při konfiguraci tohoto scénáře:

Vytvořit uživatelské certifikáty

V tomto příkladu jsou vyžadovány dva uživatelské certifikáty. Jedná se o odesílající certifikát uživatele, který je potřebný k podepsání zpráv, a certifikát uživatele příjemce, který je potřebný k zašifrování a dešifrování dat zprávy. Odesílající uživatel je 'TELLER5' a odesílající uživatel je 'FINADM2'.

Požaduje se také certifikát certifikační autority (CA).Certifikát CA je certifikát autority, která vydala certifikát uživatele. Může se jednat o řetězec certifikátů. Pokud ano, všechny certifikáty v řetězci jsou vyžadovány v svazku klíčů uživatele úlohy Advanced Message Security , v tomto případě uživatele WMQBNK6.

Certifikát CA lze vytvořit pomocí příkazu RACF RACDCERT. Tento certifikát se používá k vydávání uživatelských certifikátů. Příklad:

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('BCOCA') O('BCO') C('US'))
KEYUSAGE(CERTSIGN) WITHLABEL('BCOCA')
```

Tento příkaz RACDCERT vytvoří certifikát CA, který pak lze použít k vydání uživatelských certifikátů pro uživatele 'TELLER5' a 'FINADM2'. Příklad:

```
RACDCERT ID(TELLER5) GENCERT SUBJECTSDN(CN('Teller5') O('BCO') C('US'))
WITHLABEL('Teller5') SIGNWITH(CERTAUTH LABEL('BCOCA'))KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)
```

```
RACDCERT ID(FINADM2) GENCERT SUBJECTSDN(CN('FinAdm2') O('BCO') C('US'))
WITHLABEL('FinAdm2') SIGNWITH(CERTAUTH LABEL('BCOCA'))KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)
```

Vaše instalace bude mít postupy pro výběr nebo vytvoření certifikátu CA, stejně jako postupy pro vydávání certifikátů a jejich distribuci do příslušných systémů.

Při exportu a importu těchto certifikátů produkt Advanced Message Security vyžaduje:

- Certifikát CA (řetěz).
- Odesílající uživatelský certifikát a jeho soukromý klíč.
- Uživatelský certifikát příjemce a jeho soukromý klíč.

Pokud používáte produkt RACF, příkaz RACDCERT EXPORT lze použít k exportu certifikátů do datové sady a příkaz RACDCERT ADD lze použít k importu certifikátů z datové sady. Další informace o těchto a dalších

příkazech RACDCERT naleznete v příručce RACDCERT (Spravovat digitální certifikáty RACF) v příručce *z/OS: Security Server RACF Command Language Reference*.

Certifikáty jsou v tomto případě vyžadovány v systému z/OS , na kterém je spuštěn správce front BNK6.

Když byly certifikáty importovány do systému z/OS , na kterém běží BNK6, uživatelské certifikáty vyžadují atribut TRUST. K přidání atributu TRUST do certifikátu lze použít příkaz ALTER RACDCERT. Příklad:

```
RACDCERT ID(TELLER5) ALTER (LABEL('Teller5')) TRUST
```

```
RACDCERT ID(FINADM2) ALTER (LABEL('FinAdm2')) TRUST
```

Připojit certifikáty k příslušným kroužkům klíčů

Když byly požadované certifikáty vytvořeny nebo importovány a nastaveny jako důvěryhodné, musí být připojeny k příslušným kroužkům klíčů uživatele na systému z/OS , na kterém běží BNK6. Chcete-li vytvořit svazky klíčů, použijte příkaz RACDCERT ADDRING:

```
RACDCERT ID(WMQBNK6) ADDRING(drq.ams.keyring)
```

```
RACDCERT ID(TELLER5) ADDRING(drq.ams.keyring)
```

```
RACDCERT ID(FINADM2) ADDRING(drq.ams.keyring)
```

Tím se vytvoří svazek klíčů pro uživatele úlohy Advanced Message Security a svazky klíčů pro odesílající a přijímající uživatele. Všimněte si, že název svazku klíčů `drq.ams.keyring` je povinný a název rozlišuje velikost písmen.

Když jsou vytvořeny svazky klíčů, lze připojit příslušné certifikáty.

```
RACDCERT ID(WMQBNK6) CONNECT(CERTAUTH LABEL('BCOCA')
RING(drq.ams.keyring))
```

```
RACDCERT ID(WMQBNK6) CONNECT(ID(FINADM2) LABEL('FinAdm2')
RING(drq.ams.keyring) USAGE(SITE))
```

```
RACDCERT ID(TELLER5) CONNECT(ID(TELLER5) LABEL('Teller5')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
```

```
RACDCERT ID(FINADM2) CONNECT(ID(FINADM2) LABEL('FinAdm2')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
```

Odesílající a přijímající uživatelské certifikáty musí být připojeny jako DEFAULT. Pokud má některý uživatel ve svém drq.ams.keyringvíce než jeden certifikát, použije se výchozí certifikát pro účely podepisování a dešifrování.

Certifikát uživatele příjemce musí být také připojen ke svazku klíčů uživatele úlohy Advanced Message Security pomocí USAGE (SITE). Důvodem je skutečnost, že úloha rozšířeného zabezpečení zpráv při šifrování dat zprávy potřebuje veřejný klíč příjemce. Jednotka USAGE (SITE) zabraňuje v přístupu k soukromému klíči ve svazku klíčů.

Vytvoření a úprava certifikátů není produktem Advanced Message Security rozpoznána, dokud není správce front zastaven a restartován, nebo dokud není příkaz z/OS **MODIFY** použit k aktualizaci konfigurace certifikátu Advanced Message Security . Příklad:

```
F BNK6AMSM,REFRESH KEYRING
```

Vytvořit zásadu Advanced Message Security

V tomto příkladu jsou zprávy chráněné ochranou soukromí vkládány do fronty FIN.XFER.Q8 aplikací spuštěnou jako uživatel 'TELLER5' a načtenou ze stejné fronty aplikací spuštěnou jako uživatel 'FINADM2', takže je požadována pouze jedna zásada Advanced Message Security .

Zásady systému Advanced Message Security jsou vytvořeny pomocí obslužného programu CSQ0UTIL , který je dokumentován v tématu Obslužný program zásad zabezpečení zpráv (CSQ0UTIL).

Pomocí obslužného programu CSQ0UTIL spusťte následující příkaz:

```
setmqspl -m BNK6 -p FIN.XFER.Q8 -s SHA1 -e 3DES -a CN=Teller5,O=BCO,C=US -r
CN=FinAdm2,O=BCO,C=US
```

V této zásadě je správce front identifikován jako BNK6. Název zásady a přidružená fronta jsou FIN.XFER.Q8. Algoritmus použitý ke generování podpisu odesílatele je Deprecated SHA1a rozlišující název (DN) odesílajícího uživatele je 'CN=Teller5,O=BCO,C=US' a přijímající uživatel je 'CN=FinAdm2,O=BCO,C=US'. Algoritmus použitý k šifrování dat zprávy je Deprecated 3DES.

Po definování zásady buď restartujte správce front BNK6 , nebo pomocí příkazu z/OS **MODIFY** aktualizujte konfiguraci zásady Advanced Message Security . Příklad:

```
F BNK6AMSM,REFRESH POLICY
```

z/OS *Vzdálené řazení zpráv chráněných integritou do front pro systém AMS on z/OS*

V tomto příkladu jsou uvedeny podrobnosti o zásadách a certifikátech systému Advanced Message Security potřebných k odesílání a načítání zpráv chráněných integritou do front spravovaných dvěma různými správci front a z nich. Tito dva správci front mohou být spuštěni ve stejném systému z/OS nebo v různých systémech z/OS , nebo jeden správce front může být v distribuovaném systému se spuštěným systémem Advanced Message Security.

Příklady správců front a front jsou:

```
BNK6        - Sending queue manager
BNK7        - Recipient queue manager
FIN.XFER.Q7 - Remote queue on BNK6
FIN.RCPT.Q7 - Local queue on BNK7
```

Poznámka: V tomto příkladu jsou BNK6 a BNK7 správci front spuštěnými v různých systémech z/OS .

Používají se tito uživatelé:

```
WMQBNK6  - AMS task user on BNK6
WMQBNK7  - AMStask user on BNK7
TELLER5  - Sending user on BNK6
FINADM2  - Recipient user on BNK7
```

Postup konfigurace tohoto scénáře je následující:

Vytvořit uživatelské certifikáty

V tomto příkladu je potřeba pouze jeden uživatelský certifikát. Toto je odesílající certifikát uživatele, který je potřebný k podepsání zprávy chráněné integritou. Odesílající uživatel je 'TELLER5'.

Požaduje se také certifikát certifikační autority (CA).Certifikát CA je certifikát autority, která vydala certifikát uživatele. Může se jednat o řetězec certifikátů. Pokud ano, jsou všechny certifikáty v řetězci vyžadovány v svazku klíčů uživatele úlohy Advanced Message Security , v tomto případě uživatele WMQBNK7.

Certifikát CA lze vytvořit pomocí příkazu RACF RACDCERT. Tento certifikát se používá k vydávání uživatelských certifikátů. Příklad:

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('BCOCA') O('BCO') C('US'))
KEYUSAGE(CERTSIGN) WITHLABEL('BCOCA')
```

Tento příkaz RACDCERT vytvoří certifikát CA, který pak může být použit k vydání uživatelského certifikátu pro uživatele 'TELLER5'. Příklad:

```
RACDCERT ID(TELLER5) GENCERT SUBJECTSDN(CN('Teller5') O('BCO') C('US'))
WITHLABEL('Teller5') SIGNWITH(CERTAUTH LABEL('BCOCA'))KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)
```

Vaše instalace bude mít postupy pro výběr nebo vytvoření certifikátu CA, stejně jako postupy pro vydávání certifikátů a jejich distribuci do příslušných systémů.

Při exportu a importu těchto certifikátů produkt Advanced Message Security vyžaduje:

- Certifikát CA (řetěz).
- Odesílající uživatelský certifikát a jeho soukromý klíč.

Pokud používáte produkt RACF, příkaz RACDCERT EXPORT lze použít k exportu certifikátů do datové sady a příkaz RACDCERT ADD lze použít k importu certifikátů z datové sady. Další informace o těchto a dalších příkazech RACDCERT naleznete v příručce RACDCERT (Spravovat digitální certifikáty RACF) v příručce *z/OS: Security Server RACF Command Language Reference*.

V tomto případě jsou certifikáty vyžadovány v systému z/OS , na kterém je spuštěn správce front BNK6 a BNK7.

V tomto příkladu musí být odesílající certifikát importován do systému z/OS se systémem BNK6a certifikát CA musí být importován do systému z/OS se systémem BNK7. Když byly certifikáty importovány, uživatelský certifikát vyžaduje atribut TRUST. K přidání atributu TRUST do certifikátu lze použít příkaz ALTER RACDCERT. Například na BNK6:

```
RACDCERT ID(TELLER5) ALTER (LABEL('Teller5')) TRUST
```

Připojit certifikáty k příslušným kroužkům klíčů

Když byly požadované certifikáty vytvořeny nebo importovány a nastaveny jako důvěryhodné, musí být připojeny k příslušným uživatelským klíčům v systému z/OS , na kterém běží BNK6 a BNK7.

Chcete-li vytvořit svazky klíčů, použijte příkaz RACDCERT ADDRING na BNK6:

```
RACDCERT ID(TELLER5) ADDRING(drq.ams.keyring)
```

Tím se vytvoří svazek klíčů pro odesílajícího uživatele na serveru BNK6. Všimněte si, že název svazku klíčů drq.ams.keyring je povinný a název rozlišuje velikost písmen.

Na serveru BNK7:

```
RACDCERT ID(WMQBNK7) ADDRING(drq.ams.keyring)
```

Tím se vytvoří svazek klíčů pro uživatele úlohy Advanced Message Security na BNK7. Pro 'TELLER5' na BNK7není požadován žádný svazek klíčů uživatele.

Když jsou vytvořeny svazky klíčů, lze připojit příslušné certifikáty.

Na serveru BNK6:

```
RACDCERT ID(TELLER5) CONNECT(ID(TELLER5) LABEL('Teller5')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
```

Na serveru BNK7:

```
RACDCERT ID(WMQBNK7) CONNECT(CERTAUTH LABEL('BCOCA')
RING(drq.ams.keyring))
```

Odesílající uživatelský certifikát musí být připojen jako DEFAULT. Pokud má odesílající uživatel ve svém drq.ams.keyringvíce než jeden certifikát, použije se pro účely podepisování výchozí certifikát.

Vytvoření a úprava certifikátů není produktem Advanced Message Security rozpoznána, dokud není správce front zastaven a restartován, nebo dokud není příkaz z/OS **MODIFY** použit k aktualizaci konfigurace certifikátu Advanced Message Security . Příklad:

Na serveru BNK6:

```
F BNK6AMSM,REFRESH,KEYRING
```

Na serveru BNK7:

```
F BNK7AMSM,REFRESH,KEYRING
```

Vytvořit zásady Advanced Message Security

V tomto příkladu jsou zprávy chráněné integritou vloženy do vzdálené fronty FIN.XFER.Q7 na BNK6 aplikací spuštěnou jako uživatel 'TELLER5' a načtenou z lokální fronty FIN.RCPT.Q7 na BNK7 aplikací spuštěnou jako uživatel 'FINADM2', takže jsou vyžadovány dvě zásady Advanced Message Security .

Zásady systému Advanced Message Security jsou vytvořeny pomocí obslužného programu CSQ0UTIL , který je dokumentován v tématu Obslužný program zásad zabezpečení zpráv (CSQ0UTIL).

Obslužný program CSQ0UTIL použijte ke spuštění následujícího příkazu k definování zásady integrity pro vzdálenou frontu na serveru BNK6:

```
setmqspl -m BNK6 -p FIN.XFER.Q7 -s MD5 -a CN=Teller5,O=BCO,C=US
```

V této zásadě je správce front identifikován jako BNK6. Název zásady a přidružená fronta jsou FIN.XFER.Q7. Algoritmus použitý ke generování podpisu odesílatele je MD5a rozlišující název (DN) odesílajícího uživatele je 'CN=Teller5,O=BCO,C=US'.

Pomocí obslužného programu CSQ0UTIL můžete také spustit následující příkaz a definovat zásadu integrity pro lokální frontu v prostředí BNK7:

```
setmqspl -m BNK7 -p FIN.RCPT.Q7 -s MD5 -a CN=Teller5,O=BCO,C=US
```

V této zásadě je správce front identifikován jako BNK7. Název zásady a přidružená fronta jsou FIN.RCPT.Q7. Očekávaný algoritmus pro podpis odesílatele je MD5a očekává se, že rozlišující název (DN) odesílajícího uživatele bude 'CN=Teller5,O=BCO,C=US'.

Po definování těchto dvou zásad buď restartujte správce front BNK6 a BNK7 , nebo pomocí příkazu z/OS **MODIFY** aktualizujte konfigurace zásad Advanced Message Security . Příklad:

Na serveru BNK6:

```
F BNK6AMSM,REFRESH,POLICY
```

Na serveru BNK7:

```
F BNK7AMSM,REFRESH,POLICY
```

z/OS *Vzdálené řazení zpráv chráněných ochranou soukromí do fronty pro AMS on z/OS*

Tento příklad podrobně popisuje zásady a certifikáty Advanced Message Security potřebné k odesílání a načítání zpráv chráněných soukromím do a z front spravovaných dvěma různými správci front. Tito dva

správci front mohou být spuštěni ve stejném systému z/OS nebo v různých systémech z/OS , nebo jeden správce front může být v distribuovaném systému se spuštěným systémem Advanced Message Security.

Příklady správců front a front jsou:

```
BNK6        - Sending queue manager
BNK7        - Recipient queue manager
FIN.XFER.Q7 - Remote queue on BNK6
FIN.RCPT.Q7 - Local queue on BNK7
```

Poznámka: V tomto příkladu jsou BNK6 a BNK7 správci front běžící na různých systémech z/OS se stejným názvem.

Používají se tito uživatelé:

```
WMQBNK6  - AMS task user on BNK6
WMQBNK7  - AMS task user on BNK7
TELLER5  - Sending user on BNK6
FINADM2  - Recipient user on BNK7
```

Postup konfigurace tohoto scénáře je následující:

Vytvořit uživatelské certifikáty

V tomto příkladu jsou vyžadovány dva uživatelské certifikáty. Jedná se o odesílající certifikát uživatele, který je potřebný k podepsání zpráv, a certifikát uživatele příjemce, který je potřebný k zašifrování a dešifrování dat zprávy. Odesílající uživatel je 'TELLER5' a odesílající uživatel je 'FINADM2'.

Požaduje se také certifikát certifikační autority (CA).Certifikát CA je certifikát autority, která vydala certifikát uživatele. Může se jednat o řetězec certifikátů. Pokud ano, jsou všechny certifikáty v řetězci vyžadovány v svazku klíčů uživatele úlohy Advanced Message Security , v tomto případě uživatele WMQBNK7.

Certifikát CA lze vytvořit pomocí příkazu RACF RACDCERT. Tento certifikát se používá k vydávání uživatelských certifikátů. Příklad:

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('BCOCA') O('BCO') C('US'))
KEYUSAGE(CERTSIGN) WITHLABEL('BCOCA')
```

Tento příkaz RACDCERT vytvoří certifikát CA, který pak lze použít k vydání uživatelských certifikátů pro uživatele 'TELLER5' a 'FINADM2'. Příklad:

```
RACDCERT ID(TELLER5) GENCERT SUBJECTSDN(CN('Teller5') O('BCO') C('US'))
WITHLABEL('Teller5') SIGNWITH(CERTAUTH LABEL('BCOCA'))KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)
```

```
RACDCERT ID(FINADM2) GENCERT SUBJECTSDN(CN('FinAdm2') O('BCO') C('US'))
WITHLABEL('FinAdm2') SIGNWITH(CERTAUTH LABEL('BCOCA'))KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)
```

Vaše instalace bude mít postupy pro výběr nebo vytvoření certifikátu CA, stejně jako postupy pro vydávání certifikátů a jejich distribuci do příslušných systémů.

Při exportu a importu těchto certifikátů produkt Advanced Message Security vyžaduje:

- Certifikát CA (řetěz).
- Odesílající uživatelský certifikát a jeho soukromý klíč.
- Uživatelský certifikát příjemce a jeho soukromý klíč.

Pokud používáte produkt RACF, příkaz RACDCERT EXPORT lze použít k exportu certifikátů do datové sady a příkaz RACDCERT ADD lze použít k importu certifikátů z datové sady.

Další informace o těchto a dalších příkazech RACDCERT naleznete v příručce RACDCERT (Spravovat digitální certifikáty RACF) v příručce *z/OS: Security Server RACF Command Language Reference*.

V tomto případě jsou certifikáty vyžadovány v systému z/OS , na kterém je spuštěn správce front BNK6 a BNK7.

V tomto příkladu musí být odesílající a přijímající certifikáty importovány do systému z/OS se systémem BNK6a certifikační autorita a certifikáty příjemce musí být importovány do systému z/OS se systémem BNK7. Když byly certifikáty importovány, uživatelské certifikáty vyžadují atribut TRUST. K přidání atributu TRUST do certifikátu lze použít příkaz ALTER RACDCERT. Příklad:

Na serveru BNK6:

```
RACDCERT ID(TELLER5) ALTER (LABEL('Teller5')) TRUST
```

```
RACDCERT ID(FINADM2) ALTER (LABEL('FinAdm2')) TRUST
```

Na serveru BNK7:

```
RACDCERT ID(FINADM2) ALTER (LABEL('FinAdm2')) TRUST
```

Připojit certifikáty k příslušným kroužkům klíčů

Když byly požadované certifikáty vytvořeny nebo importovány a nastaveny jako důvěryhodné, musí být připojeny k příslušným uživatelským klíčům na systémech z/OS , na kterých běží BNK6 a BNK7.

Chcete-li vytvořit svazky klíčů, použijte příkaz RACDCERT ADDRING:

Na serveru BNK6:

```
RACDCERT ID(WMQBNK6) ADDRING(drq.ams.keyring)
```

```
RACDCERT ID(TELLER5) ADDRING(drq.ams.keyring)
```

Tím se vytvoří svazek klíčů pro uživatele úlohy Advanced Message Security a svazek klíčů pro odesílajícího uživatele na serveru BNK6. Všimněte si, že název svazku klíčů drq.ams.keyring je povinný a název rozlišuje velikost písmen.

Na serveru BNK7:

```
RACDCERT ID(WMQBNK7) ADDRING(drq.ams.keyring)
```

```
RACDCERT ID(FINADM2) ADDRING(drq.ams.keyring)
```

Tím se vytvoří svazek klíčů pro uživatele úlohy Advanced Message Security a svazek klíčů pro uživatele příjemce na serveru BNK7.

Když jsou vytvořeny svazky klíčů, lze připojit příslušné certifikáty.

Na serveru BNK6:

```
RACDCERT ID(WMQBNK6) CONNECT(ID(FINADM2) LABEL('FinAdm2')
RING(drq.ams.keyring) USAGE(SITE))
```

```
RACDCERT ID(TELLER5) CONNECT(ID(TELLER5) LABEL('Teller5')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
```

Na serveru BNK7:

```
RACDCERT ID(WMQBNK7) CONNECT(CERTAUTH LABEL('BCOCA')
RING(drq.ams.keyring))
```

```
RACDCERT ID(FINADM2) CONNECT(ID(FINADM2) LABEL('FinAdm2')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
```

Odesílající a přijímající uživatelské certifikáty musí být připojeny jako DEFAULT. Pokud má některý uživatel ve svém drq.ams.keyringvíce než jeden certifikát, použije se výchozí certifikát pro účely podepisování a šifrování/dešifrování.

V systému BNK6musí být certifikát uživatele příjemce také připojen ke svazku klíčů uživatele úlohy Advanced Message Security pomocí USAGE (SITE). Důvodem je skutečnost, že úloha rozšířeného zabezpečení zpráv při šifrování dat zprávy potřebuje veřejný klíč příjemce. Jednotka USAGE (SITE) zabraňuje v přístupu k soukromému klíči ve svazku klíčů.

Vytvoření a úprava certifikátů není produktem Advanced Message Security rozpoznána, dokud není správce front zastaven a restartován, nebo dokud není příkaz z/OS **MODIFY** použit k aktualizaci konfigurace certifikátu Advanced Message Security . Příklad:

Na serveru BNK6:

```
F BNK6AMSM,REFRESH,KEYRING
```

Na serveru BNK7:

```
F BNK7AMSM,REFRESH,KEYRING
```

Vytvořit zásady Advanced Message Security

V tomto příkladu jsou zprávy chráněné ochranou soukromí vkládány do vzdálené fronty FIN.XFER.Q7 na BNK6 aplikací spuštěnou jako uživatel 'TELLER5' a načtenou z lokální fronty FIN.RCPT.Q7 na BNK7 aplikací spuštěnou jako uživatel 'FINADM2', takže jsou vyžadovány dvě zásady Advanced Message Security .

Zásady systému Advanced Message Security jsou vytvořeny pomocí obslužného programu CSQ0UTIL , který je dokumentován v tématu Obslužný program zásad zabezpečení zpráv (CSQ0UTIL).

Pomocí obslužného programu CSQ0UTIL spusťte následující příkaz a definujte zásady ochrany osobních údajů pro vzdálenou frontu na serveru BNK6:

```
setmqspl -m BNK6 -p FIN.XFER.Q7 -s SHA1 -e 3DES -a CN=Teller5,O=BCO,C=US -r
CN=FinAdm2,O=BCO,C=US
```

V této zásadě je správce front identifikován jako BNK6. Název zásady a přidružená fronta jsou FIN.XFER.Q7. Algoritmus použitý ke generování podpisu odesílatele je Deprecated SHA1, rozlišující název (DN) odesílajícího uživatele je 'CN=Teller5,O=BCO,C=US' a přijímající uživatel je 'CN=FinAdm2,O=BCO,C=US'. Algoritmus použitý k šifrování dat zprávy je Deprecated 3DES.

Pomocí obslužného programu CSQ0UTIL můžete také spustit následující příkaz a definovat zásady ochrany osobních údajů pro lokální frontu v systému BNK7:

```
setmqspl -m BNK7 -p FIN.RCPT.Q7 -s SHA1 -e 3DES -a CN=Teller5,O=BCO,C=US -r
CN=FinAdm2,O=BCO,C=US
```

V této zásadě je správce front identifikován jako BNK7. Název zásady a přidružená fronta jsou FIN.RCPT.Q7. Očekávaný algoritmus pro podpis odesílatele je Deprecated SHA1, očekává se, že rozlišující název (DN) odesílajícího uživatele bude 'CN=Teller5,O=BCO,C=US' a uživatel příjemce je 'CN=FinAdm2,O=BCO,C=US'. Algoritmus použitý k dešifrování dat zprávy je Deprecated 3DES.

Po definování těchto dvou zásad buď restartujte správce front BNK6 a BNK7 , nebo pomocí příkazu z/OS **MODIFY** aktualizujte konfiguraci zásad Advanced Message Security . Příklad:

Na serveru BNK6:

```
F BNK6AMSM,REFRESH,POLICY
```

Na serveru BNK7:

```
F BNK7AMSM,REFRESH,POLICY
```

Stručná úvodní příručka pro klienty AMS with Java

Tato příručka slouží k rychlé konfiguraci produktu Advanced Message Security tak, aby poskytoval zabezpečení zpráv pro aplikace Java , které se připojují pomocí vazeb klienta. V době, kdy jej dokončíte, budete mít vytvořeno úložiště klíčů pro ověření identit uživatelů a definované zásady podepisování a šifrování pro vašeho správce front.

Než začnete

Ujistěte se, že máte nainstalované příslušné komponenty, jak je popsáno v **Stručné úvodní příručce** (Windows nebo AIX and Linux).

1. Vytvoření správce front a fronty

Informace o této úloze

Všechny následující příklady používají frontu s názvem TEST.Q pro předávání zpráv mezi aplikacemi. Produkt Advanced Message Security používá zachytávače k podepisování a šifrování zpráv v okamžiku, kdy vstoupí do infrastruktury IBM MQ prostřednictvím standardního rozhraní IBM MQ . Základní nastavení se provádí v produktu IBM MQ a konfiguruje se v následujících krocích.

Postup

1. Vytvoření správce front

   ```
   crtmqm QM_VERIFY_AMS
   ```

2. Spustit správce front

   ```
   strmqm QM_VERIFY_AMS
   ```

3. Vytvořte a spusťte modul listener zadáním následujících příkazů do adresáře **runmqsc** pro správce front QM_VERIFY_AMS .

   ```
   DEFINE LISTENER(AMS.LSTR) TRPTYPE(TCP) PORT(1414) CONTROL(QMGR)
   ```

   ```
   START LISTENER(AMS.LSTR)
   ```

4. Vytvořte kanál pro připojení našich aplikací zadáním následujícího příkazu do adresáře **runmqsc** pro správce front QM_VERIFY_AMS .

   ```
   DEFINE CHANNEL(AMS.SVRCONN) CHLTYPE(SVRCONN)
   ```

5. Vytvořte frontu s názvem TEST.Q zadáním následujícího příkazu do adresáře **runmqsc** pro správce front QM_VERIFY_AMS .

   ```
   DEFINE QLOCAL(TEST.Q)
   ```

Výsledky

Pokud byla procedura úspěšně dokončena, následující příkaz zadaný do adresáře **runmqsc** zobrazí podrobnosti o souboru TEST.Q:

```
DISPLAY Q(TEST.Q)
```

2. Vytvoření a autorizace uživatelů

Informace o této úloze

V tomto scénáři se objevují dva uživatelé: `alice`, odesilatel a bob, příjemce. Chcete-li používat frontu aplikací, těmto uživatelům musí být uděleno oprávnění k jejímu použití. Také pro úspěšné použití zásad ochrany definovaných v tomto scénáři musí být těmto uživatelům udělen přístup k některým systémovým frontám. Další informace o příkazu **setmqaut** viz **setmqaut**.

Postup

1. Vytvořte dva uživatele, jak je popsáno v **Stručné úvodní příručce** (Windows nebo AIX and Linux) pro vaši platformu.
2. Autorizovat uživatele pro připojení ke správci front a pro práci s frontou

   ```
   setmqaut -m QM_VERIFY_AMS -t qmgr -p alice -p bob +connect +inq
   ```

   ```
   setmqaut -m QM_VERIFY_AMS -n TEST.Q -t queue -p alice +put
   ```

   ```
   setmqaut -m QM_VERIFY_AMS -n TEST.Q -t queue -p bob +get +inq +browse
   ```

3. Měli byste také umožnit oběma uživatelům procházet frontu systémových zásad a vkládat zprávy do fronty chyb.

   ```
   setmqaut -m QM_VERIFY_AMS -t queue -n SYSTEM.PROTECTION.POLICY.QUEUE -p alice -p bob +browse
   ```

   ```
   setmqaut -m QM_VERIFY_AMS -t queue -n SYSTEM.PROTECTION.ERROR.QUEUE -p alice -p bob +put
   ```

   Upozornění: Produkt IBM MQ optimalizuje výkon ukládáním zásad do mezipaměti, abyste nemuseli procházet záznamy a hledat podrobnosti o zásadách v systému SYSTEM.PROTECTION.POLICY.QUEUE ve všech případech.

   Produkt IBM MQ neukládá všechny dostupné zásady do mezipaměti. Pokud existuje vysoký počet zásad, produkt IBM MQ uloží do mezipaměti omezený počet zásad. Pokud má tedy správce front definován nízký počet zásad, není třeba systému SYSTEM.PROTECTION.POLICY.QUEUE.

   Měli byste však udělit oprávnění k procházení této fronty v případě, že je definován vysoký počet zásad nebo pokud používáte staré klienty. Systém SYSTEM.PROTECTION.ERROR.QUEUE se používá k vložení chybových zpráv generovaných kódem AMS. Oprávnění vložení pro tuto frontu je kontrolováno pouze při pokusu o vložení chybové zprávy do fronty. Vaše oprávnění pro vložení do fronty není kontrolováno, když se pokusíte vložit nebo získat zprávu z chráněné fronty AMS.

Výsledky

Nyní jsou uživatelé vytvořeni a jsou jim udělena požadovaná oprávnění.

Jak pokračovat dále

Chcete-li ověřit, zda byly kroky provedeny správně, použijte ukázky `JmsProducer` a `JmsConsumer` , jak je popsáno v části “7. Testování nastavení” na stránce 649.

3. Vytvoření databáze klíčů a certifikátů

Informace o této úloze

Šifrování zprávy zachytávači vyžaduje veřejný klíč odesílajících uživatelů. Proto musí být vytvořena databáze klíčů identit uživatelů mapovaných na veřejné a soukromé klíče. V reálném systému, kde jsou uživatelé a aplikace rozptýleny na několika počítačích, by měl každý uživatel své vlastní soukromé úložiště klíčů. Podobně v této příručce vytváříme databáze klíčů pro `alice` a bob a sdílíme mezi nimi uživatelské certifikáty.

Poznámka: V této příručce používáme ukázkové aplikace napsané v části Java , které se připojují pomocí vazeb klienta. Pokud plánujete používat aplikace Java používající lokální vazby nebo aplikace v jazyce C, musíte vytvořit úložiště klíčů a certifikáty systému CMS pomocí příkazu **runmqakm** . Zobrazí se v **stručné úvodní příručce** (Windows nebo AIX and Linux).

Postup

1. Vytvořte adresář, ve kterém se má vytvořit úložiště klíčů, například `/home/alice/.mqs`. Můžete jej vytvořit ve stejném adresáři, který používá **Stručná úvodní příručka** (Windows nebo AIX and Linux) pro vaši platformu.

   Poznámka: Na tento adresář se v následujících krocích odkazuje jako na *keystore-dir* .
2. Vytvořte nové úložiště klíčů a certifikát identifikující uživatele `alice` pro použití v šifrování

   Poznámka: Příkaz **keytool** je součástí prostředí JRE.

   ```
   keytool -genkey -alias Alice_Java_Cert -keyalg RSA -keystore keystore-dir/keystore.jks
   -storepass passw0rd
   -dname "CN=alice, O=IBM, C=GB" -keypass passw0rd
   ```

   Poznámka:

   - Pokud váš *keystore-dir* obsahuje mezery, musíte uzavřít celý název úložiště klíčů do uvozovek.
   - K zabezpečení úložiště klíčů se doporučuje použít silné heslo.
   - Pro účely této příručky používáme certifikát podepsaný svým držitelem, který lze vytvořit bez použití certifikační autority. U produkčních systémů se doporučuje nepoužívat certifikáty podepsané svým držitelem, ale spoléhat se na certifikáty podepsané certifikační autoritou.
   - Parametr **alias** určuje název certifikátu, který zachytávače vyhledají, aby obdržely nezbytné informace.
   - Parametr **dname** uvádí podrobnosti o **rozlišujícím názvu** (DN), který musí být pro každého uživatele jedinečný.
3. V systému AIX and Linuxse ujistěte, že je úložiště klíčů čitelné.

   ```
   chmod +r keystore-dir/keystore.jks
   ```
4. Opakujte step1-4 pro uživatele bob

Výsledky

Oba uživatelé `alice` a bob mají nyní certifikát podepsaný svým držitelem.

4. Vytvoření souboru keystore.conf

Informace o této úloze

Musíte odvést zachytávače Advanced Message Security do adresáře, kde jsou umístěny databáze klíčů a certifikáty. To se provádí prostřednictvím souboru `keystore.conf` , který obsahuje tyto informace ve formátu prostého textu. Každý uživatel musí mít samostatný soubor `keystore.conf` . Tento krok by měl být proveden pro `alice` i bob.

Příklad

Pro tento scénář je obsah `keystore.conf` pro `alice` následující:

```
JKS.keystore = keystore-dir/keystore
JKS.certificate = Alice_Java_Cert
JKS.encrypted = no
JKS.keystore_pass = passw0rd
JKS.key_pass = passw0rd
JKS.provider = IBMJCE
```

Pro tento scénář je obsah `keystore.conf` pro bob následující:

```
JKS.keystore = keystore-dir/keystore
JKS.certificate = Bob_Java_Cert
JKS.encrypted = no
JKS.keystore_pass = passw0rd
JKS.key_pass = passw0rd
JKS.provider = IBMJCE
```

Poznámka:

- Cesta k souboru úložiště klíčů musí být poskytnuta bez přípony souboru.
- Pokud již máte soubor `keystore.conf` , protože jste postupovali podle pokynů v stručné úvodní příručce (Windows nebo AIX and Linux), můžete upravit existující soubor a přidat tyto řádky.
- Další informace viz téma “Struktura konfiguračního souboru úložiště klíčů (keystore.conf) pro AMS” na stránce 658.

5. Sdílení certifikátů

Informace o této úloze

Sdílejte certifikáty mezi těmito dvěma úložišti klíčů, aby každý uživatel mohl úspěšně identifikovat druhého. To se provádí extrahováním certifikátu každého uživatele a jeho importem do úložiště klíčů jiného uživatele.

Poznámka: Výrazy *extract* a *export* se používají odlišně různými certifikačním nástroji. Například nástroj IBM Global Security Kit (GSKit) **strmqikm** (ikeyman) rozlišuje, že *extrahujete* certifikáty (veřejné klíče) a *exportujete* soukromé klíče. Tento rozdíl je velmi důležitý pro nástroje, které nabízejí obě možnosti, protože použití *exportu* by omylem zcela ohrozilo vaši aplikaci předáním jejího soukromého klíče. Vzhledem k tomu, že rozlišení je tak důležité, dokumentace IBM MQ se snaží používat tyto výrazy konzistentně. Nástroj keytool Java však poskytuje volbu příkazového řádku s názvem *exportcert* , která extrahuje pouze veřejný klíč. Z těchto důvodů se následující procedura odkazuje na *extrakci* certifikátů pomocí volby *exportcert* .

Postup

1. Extrahujte certifikát identifikující `alice`.

   ```
   keytool -exportcert -keystore alice-keystore-dir/keystore.jks -storepass passw0rd
   -alias Alice_Java_Cert -file alice-keystore-dir/Alice_Java_Cert.cer
   ```

2. Importujte certifikát identifikující `alice` do úložiště klíčů, které bude produkt bob používat. Když jste vyzváni, označte, že budete důvěřovat tomuto certifikátu.

```
keytool -importcert -file alice-keystore-dir/Alice_Java_Cert.cer -alias Alice_Java_Cert
-keystore bob-keystore-dir/keystore.jks -storepass passw0rd
```

3. Zopakujte kroky pro bob

Výsledky

Dva uživatelé `alice` a bob se nyní mohou úspěšně identifikovat, zda vytvořili a sdíleli certifikáty podepsané sebou samým.

Jak pokračovat dále

Ověřte, že je certifikát v úložišti klíčů, spuštěním následujících příkazů, které vytisknou jeho podrobnosti:

```
keytool -list -keystore bob-keystore-dir/keystore.jks -storepass passw0rd -alias Alice_Java_Cert
```

```
keytool -list -keystore alice-keystore-dir/keystore.jks -storepass passw0rd -alias Bob_Java_Cert
```

6. Definování zásady fronty

Informace o této úloze

S vytvořeným správcem front a zachytávači připravenými k zachycení zpráv a přístupu k šifrovacím klíčům můžeme začít definovat zásady ochrany v systému `QM_VERIFY_AMS` pomocí příkazu `setmqspl` . Další informace o tomto příkazu viz setmqspl . Každý název zásady musí být stejný jako název fronty, na kterou se má použít.

Příklad

Toto je příklad zásady definované ve frontě `TEST.Q` , podepsané uživatelem `alice` pomocí algoritmu Deprecated SHA1 a šifrované pomocí 256bitového algoritmu AES pro uživatele bob:

```
setmqspl -m QM_VERIFY_AMS -p TEST.Q -s SHA1 -a "CN=alice,O=IBM,C=GB" -e AES256 -r
"CN=bob,O=IBM,C=GB"
```

Poznámka: DN se přesně shodují s těmi, která jsou uvedena v příslušném certifikátu uživatele z databáze klíčů.

Jak pokračovat dále

Chcete-li ověřit zásadu, kterou jste definovali, zadejte následující příkaz:

```
dspmqspl -m QM_VERIFY_AMS
```

Chcete-li vytisknout podrobnosti o zásadě jako sadu příkazů `setmqspl` , použijte příznak `-export` . To umožňuje ukládání již definovaných zásad:

```
dspmqspl -m QM_VERIFY_AMS -export >restore_my_policies.bat
```

7. Testování nastavení

Než začnete

Ujistěte se, že verze produktu Java , kterou používáte, má nainstalované neomezené soubory zásad JCE.

Poznámka: Verze produktu Java dodaná v instalaci produktu IBM MQ již má tyto soubory zásad. Je k dispozici v adresáři *MQ_INSTALLATION_PATH*/java/bin.

Informace o této úloze

Spuštěním různých programů pod různými uživateli můžete ověřit, zda byla aplikace správně nakonfigurována. Podrobnosti o spouštění programů pod různými uživateli viz **Stručná úvodní příručka** (Windows nebo AIX) pro vaši platformu.

Postup

1. Chcete-li spustit tyto ukázkové aplikace JMS , použijte nastavení CLASSPATH pro vaši platformu, jak je uvedeno v části Proměnné prostředí používané produktem IBM MQ classes for JMS , abyste se ujistili, že je zahrnut adresář ukázek.
2. Jako uživatel `alice`vložte zprávu pomocí ukázkové aplikace, připojující se jako klient:

```
java JmsProducer -m QM_VERIFY_AMS -d TEST.Q -h localhost -p 1414 -l AMS.SVRCONN
```

3. Jako uživatel bobzískejte zprávu pomocí ukázkové aplikace, která se připojuje jako klient:

```
java JmsConsumer -m QM_VERIFY_AMS -d TEST.Q -h localhost -p 1414 -l AMS.SVRCONN
```

Výsledky

Pokud byla aplikace správně nakonfigurována pro oba uživatele, zobrazí se zpráva uživatele `alice` , když produkt bob spustí získávanou aplikaci.

Ochrana vzdálených front v systému AMS

Chcete-li plně chránit vzdálené fronty, musí být ve vzdálené frontě a lokální frontě, do které jsou zprávy přenášeny, nastaveny zásady.

Když je zpráva vložena do vzdálené fronty, produkt Advanced Message Security zachytí operaci a zpracuje zprávu podle sady zásad pro vzdálenou frontu. Například pro zásadu šifrování je zpráva zašifrována před jejím předáním do IBM MQ , aby ji zpracovala. Poté, co produkt Advanced Message Security zpracuje zprávu vloženou do vzdálené fronty, produkt IBM MQ ji vloží do přidružené přenosové fronty a předá ji správci cílové fronty a cílové frontě.

Když je v lokální frontě provedena operace GET, produkt Advanced Message Security se pokusí dekódovat zprávu podle sady zásad v lokální frontě. Aby byla operace úspěšná, musí být zásada použitá k dešifrování zprávy identická se zásadou použitou k jejímu zašifrování. Jakýkoli nesoulad způsobí odmítnutí zprávy.

Pokud z nějakého důvodu nelze obě zásady nastavit současně, je poskytnuta podpora fázovaného zavedení. Zásadu lze nastavit v lokální frontě s příznakem tolerance, který označuje, že zásadu přidruženou k frontě lze ignorovat, když se pokus o načtení zprávy z fronty týká zprávy, která nemá nastavenou sadu zásad zabezpečení. V tomto případě se příkaz GET pokusí zprávu dešifrovat, ale umožní doručení nešifrovaných zpráv. Tímto způsobem lze nastavit zásady ve vzdálených frontách poté, co byly lokální fronty chráněny (a testovány).

Zapamatujte si: Po dokončení zavedení systému Advanced Message Security odeberte příznak tolerance.

Související odkazy

setmqspl (nastavit zásadu zabezpečení)

Směrování chráněných zpráv pomocí AMS použití IBM Integration Bus

Produkt Advanced Message Security může chránit zprávy v infrastruktuře, kde je nainstalován produkt IBM Integration Busnebo WebSphere Message Broker 8.0.0.1 (nebo novější). Před použitím zabezpečení v prostředí IBM Integration Bus byste měli porozumět povaze obou produktů.

Informace o této úloze

Produkt Advanced Message Security poskytuje komplexní zabezpečení informačního obsahu zprávy. To znamená, že pouze strany uvedené jako platné odesilatele a příjemce zprávy jsou schopny zprávu vytvořit nebo přijmout. To znamená, že chcete-li zabezpečit zprávy procházející produktem IBM Integration Bus, můžete buď povolit produktu IBM Integration Bus zpracovávat zprávy bez znalosti jejich obsahu (Scénář 1). nebo jej učiňte oprávněným uživatelem schopným přijímat a odesílat zprávy (Scénář 2).

Scénář 1- Integration Bus nemůže zobrazit obsah zprávy

Než začnete

Produkt IBM Integration Bus by měl být připojen k existujícímu správci front. Řetězec *QMgrName* nahraďte tímto existujícím názvem správce front v následujících příkazech.

Informace o této úloze

V tomto scénáři Alice vloží chráněnou zprávu do vstupní fronty `QIN`. Na základě vlastnosti zprávy `route`Toje zpráva směrována do *bob's* (`QBOB`),[1](`QCECIL`), nebo výchozí (`QDEF`) fronta. Směrování je možné, protože produkt Advanced Message Security chrání pouze informační obsah zprávy, nikoli jeho záhlaví a vlastnosti, které zůstávají nechráněné a může je číst produkt IBM Integration Bus. Advanced Message Security používají pouze *alice*, *bob* a *cecil*. Není nutné ji instalovat nebo konfigurovat pro IBM Integration Bus.

Produkt IBM Integration Bus přijme chráněnou zprávu z fronty nechráněných aliasů, aby se zabránilo jakémukoli pokusu o dešifrování zprávy. Pokud by měla používat chráněnou frontu přímo, byla by zpráva vložena do fronty DEAD LETTER, protože by ji nebylo možné dešifrovat. Zpráva je směrována produktem IBM Integration Bus a dorazí do cílové fronty beze změny. Proto je stále podepsán původním autorem (jak *bob* , tak *cecil* přijímají pouze zprávy odeslané *alice*). a chráněna jako dříve (číst ji mohou pouze *bob* a *cecil*). Produkt IBM Integration Bus vloží směrovanou zprávu do nechráněného aliasu. Příjemci načtou zprávu z chráněné výstupní fronty, kde AMS transparentně dešifruje zprávu.

Postup

1. Nakonfigurujte *alice*, *bob* a *cecil* pro použití Advanced Message Security , jak je popsáno v **stručné úvodní příručce** (Windows nebo AIX).

   Ujistěte se, že jsou dokončeny následující kroky:

   - Vytváření a autorizace uživatelů
   - Vytvoření databáze klíčů a certifikátů
   - Vytvoření souboru keystore.conf
2. Poskytněte certifikát *alice* pro *bob* a *cecil*, aby mohly být identifikovány *alice* při kontrole digitálních podpisů na zprávách.

   To provedete extrakcí certifikátu identifikujícího *alice* do externího souboru a následným přidáním extrahovaného certifikátu do úložišť klíčů *bob* a *cecil* . Je důležité, abyste použili metodu popsanou v části **Úloha 5. Sdílení certifikátů** v **stručné úvodní příručce** (Windows nebo AIX).
3. Poskytněte certifikáty *bob* a *cecil's* pro *alice*, aby *alice* mohla odesílat zprávy šifrované pro *bob* a *cecil*.

   Proveďte to pomocí metody uvedené v předchozím kroku.
4. Ve správci front definujte lokální fronty s názvem `QIN`, `QBOB`, `QCECIL` a `QDEF`.

   ```
   DEFINE QLOCAL(QIN)
   ```
5. Nastavte zásadu zabezpečení pro frontu `QIN` na vhodnou konfiguraci. Použijte stejné nastavení pro fronty `QBOB`, `QCECIL` a `QDEF` .

[1] cecil's (speciální)

```
setmqspl -m QMgrName -p QIN -s SHA1 -a "CN=alice,O=IBM,C=GB"
-e AES256 -r "CN=bob,O=IBM,C=GB" -r "CN=cecil,O=IBM,C=GB"
```

Tento scénář předpokládá zásadu zabezpečení, kde *alice* je jediným autorizovaným odesilatelem a *bob* a *cecil* jsou příjemci.

6. Definujte alias fronty AIN, ABOB a ACECIL odkazující na lokální fronty QIN, QBOB a QCECIL .

```
DEFINE QALIAS(AIN) TARGET(QIN)
```

7. Ověřte, že konfigurace zabezpečení pro aliasy určené v předchozím kroku není přítomna; jinak nastavte její zásadu na hodnotu NONE.

```
dspmqspl -m QMgrName -p AIN
```

8. V produktu IBM Integration Bus vytvořte tok zpráv pro směrování zpráv přicházejících do alias fronty AIN na uzel BOB, CECIL nebo DEF v závislosti na vlastnosti routeTo zprávy. Chcete-li tak učinit, postupujte takto:
   a) Vytvořte uzel MQInput s názvem IN a přiřaďte alias AIN jako jeho název fronty.
   b) Vytvořte uzly MQOutput s názvem BOB, CECIL a DEFa přiřaďte alias fronty ABOB, ACECIL a ADEF jako jejich názvy front.
   c) Vytvořte uzel trasy a nazvějte jej TEST.
   d) Připojte uzel IN ke vstupnímu terminálu uzlu TEST .
   e) Vytvořte výstupní terminály boba cecil pro uzel TEST .
   f) Připojte výstupní terminál bob k uzlu BOB .
   g) Připojte výstupní terminál cecil k uzlu CECIL .
   h) Připojte uzel DEF k výchozímu výstupnímu terminálu.
   i) Použijte následující pravidla:

```
$Root/MQRFH2/usr/routeTo/text()="bob"
```

```
$Root/MQRFH2/usr/routeTo/text()="cecil"
```

9. Implementujte tok zpráv do běhové komponenty IBM Integration Bus .
10. Spuštění jako uživatel Alice vloží zprávu, která obsahuje také vlastnost zprávy s názvem routeTo s hodnotou bob nebo cecil. Spuštění ukázkové aplikace **amqsstm** vám to umožní.

```
Sample AMQSSTMA start
target queue is TEST.Q
Enter property name
routeTo
Enter property value
bob
Enter property name

Enter message text
My Message to Bob
Sample AMQSSTMA end
```

11. Spuštění jako uživatel *bob* načte zprávu z fronty QBOB pomocí ukázkové aplikace **amqsget**.

Výsledky

Když *alice* vloží zprávu do fronty QIN , je zpráva chráněna. Je načten v chráněném formátu pomocí IBM Integration Bus z alias fronty AIN . Produkt IBM Integration Bus se rozhodne, kam se má směrovat zpráva, která čte vlastnost routeTo , která není jako všechny vlastnosti šifrována. Produkt

IBM Integration Bus umístí zprávu na příslušný nechráněný alias, aby se vyhnul jeho další ochraně. Když je zpráva přijata příkazem *bob* nebo *cecil* z fronty, je dešifrována a digitální podpis je ověřen.

Scénář 2- Integration Bus může zobrazit obsah zprávy

Informace o této úloze

V tomto scénáři může skupina jednotlivců odesílat zprávy do produktu IBM Integration Bus. Jiná skupina má oprávnění přijímat zprávy vytvořené produktem IBM Integration Bus. Přenos mezi stranami a produktem IBM Integration Bus nelze odposlouchat.

Nezapomeňte, že produkt IBM Integration Bus čte zásady ochrany a certifikáty pouze při otevření fronty, takže musíte prováděcí skupinu znovu načíst po provedení aktualizací zásad ochrany, aby se změny projevily.

```
mqsireload execution-group-name
```

Pokud je produkt IBM Integration Bus považován za autorizovanou stranu, která má povoleno číst nebo podepisovat informační obsah zprávy, musíte nakonfigurovat produkt Advanced Message Security pro uživatele, který spouští službu IBM Integration Bus . Uvědomte si, že to nemusí být nutně stejný uživatel, který vkládá/získává zprávy do front, ani uživatel, který vytváří a implementuje aplikace IBM Integration Bus .

Postup

1. Nakonfigurujte *alice*, *bob*, *cecil* a *dave* a uživatele služby IBM Integration Bus pro použití Advanced Message Security , jak je popsáno v **Stručné úvodní příručce** (Windows nebo AIX).

   Ujistěte se, že jsou dokončeny následující kroky:

   - Vytváření a autorizace uživatelů
   - Vytvoření databáze klíčů a certifikátů
   - Vytvoření souboru keystore.conf
2. Poskytněte uživateli služby IBM Integration Bus certifikáty *alice*, *bob*, *cecil* a *dave's* .

   To provedete extrahováním jednotlivých certifikátů identifikujících *alice*, *bob*, *cecil* a *dave* do externích souborů a následným přidáním extrahovaných certifikátů do úložiště klíčů IBM Integration Bus .
   Je důležité, abyste použili metodu popsanou v části **Úloha 5. Sdílení certifikátů** v **stručné úvodní příručce** (Windows nebo AIX).
3. Poskytněte certifikát uživatele služby IBM Integration Bus pro *alice*, *bob*, *cecil* a *dave*.

   Proveďte to pomocí metody uvedené v předchozím kroku.

   Poznámka: *Alice* a *bob* potřebují certifikát uživatele služby IBM Integration Bus pro správné šifrování zpráv. Uživatel služby IBM Integration Bus potřebuje *alice's* a *bob's* certifikáty k ověření autorů zpráv. Uživatel služby IBM Integration Bus potřebuje certifikáty *cecil's* a *dave's* , aby pro ně zašifroval zprávy. *cecil* a *dave* potřebují certifikát uživatele služby IBM Integration Bus k ověření, zda zpráva pochází z IBM Integration Bus.
4. Definujte lokální frontu s názvem IN a definujte zásadu zabezpečení s *alice* a *bob* určenými jako autoři a uživatele služby pro IBM Integration Bus určené jako příjemce:

   ```
   setmqspl -m QMgrName -p IN -s MD5 -a "CN=alice,O=IBM,C=GB" -a "CN=bob,O=IBM,C=GB"
   -e AES256 -r "CN=broker,O=IBM,C=GB"
   ```
5. Definujte lokální frontu s názvem OUTa definujte zásadu zabezpečení s uživatelem služby pro IBM Integration Bus určenou jako autor a *cecil* a *dave* určené jako příjemci:

   ```
   setmqspl -m QMgrName -p OUT -s MD5 -a "CN=broker,O=IBM,C=GB" -e AES256
   -r "CN=cecil,O=IBM,C=GB" -r "CN=dave,O=IBM,C=GB"
   ```

6. V produktu IBM Integration Bus vytvořte tok zpráv s uzlem `MQInput` a uzlem `MQOutput` . Nakonfigurujte uzel `MQInput` pro použití fronty `IN` a uzel `MQOutput` pro použití fronty `OUT` .
7. Implementujte tok zpráv do běhové komponenty IBM Integration Bus .
8. Spuštění jako uživatel *alice* nebo *bob* vloží zprávu do fronty `IN` pomocí ukázkové aplikace **amqsput**.
9. Spuštění jako uživatel *cecil* nebo *dave* načte zprávu z fronty `OUT` pomocí ukázkové aplikace **amqsget**.

Výsledky

Zprávy odeslané pomocí *alice* nebo *bob* do vstupní fronty `IN` jsou šifrovány, což umožňuje IBM Integration Bus pouze číst. IBM Integration Bus přijímá pouze zprávy z *alice* a *bob* a odmítá ostatní. Přijaté zprávy jsou odpovídajícím způsobem zpracovány, podepsány a zašifrovány pomocí klíčů *cecil's* a *dave's* před jejich vložením do výstupní fronty `OUT`. Číst lze pouze položky *cecil* a *dave* , zprávy nepodepsané IBM Integration Bus jsou odmítnuty.

Použití Advanced Message Security s Managed File Transfer

Tento scénář vysvětluje, jak nakonfigurovat produkt Advanced Message Security tak, aby poskytoval soukromí zpráv pro data odesílaná prostřednictvím produktu Managed File Transfer.

Než začnete

Ujistěte se, že máte komponentu Advanced Message Security nainstalovanou v instalaci produktu IBM MQ , která je hostitelem front používaných produktem Managed File Transfer , které chcete chránit.

Pokud se vaši agenti Managed File Transfer připojují v režimu vazeb, ujistěte se, že máte také nainstalovanou komponentu IBM Global Security Kit (GSKit) v lokální instalaci.

Informace o této úloze

Při přerušení přenosu dat mezi dvěma agenty Managed File Transfer mohou důvěrná data zůstat nechráněná v základních frontách systému IBM MQ , které se používají ke správě přenosu. Tento scénář vysvětluje, jak nakonfigurovat a používat produkt Advanced Message Security k ochraně takových dat ve frontách systému Managed File Transfer .

V tomto scénáři uvažujeme jednoduchou topologii zahrnující jeden počítač se dvěma frontami Managed File Transfer a dvěma agenty `AGENT1` a `AGENT2`, kteří sdílejí jednoho správce front, jak je popsáno ve scénáři Managed File Transfer scénář. Oba agenti se připojují stejným způsobem, buď v režimu vazeb, nebo v režimu klienta.

1. Vytvoření certifikátů

Než začnete

Tento scénář používá jednoduchý model, ve kterém se ke spuštění procesů Managed File Transfer Agent používá uživatel `ftagent` ve skupině `FTAGENTS` . Pokud používáte vlastní názvy uživatelů a skupin, změňte odpovídajícím způsobem příkazy.

Informace o této úloze

Produkt Advanced Message Security používá šifrování pomocí veřejného klíče k podepisování a/nebo šifrování zpráv v chráněných frontách.

Poznámka:

- Pokud jsou agenti Managed File Transfer spuštěni v režimu vazeb, příkazy, které použijete k vytvoření úložiště klíčů CMS (Cryptographic Message Syntax), jsou podrobně popsány v **Stručné úvodní příručce** (Windows nebo AIX) pro vaši platformu.
- Pokud jsou vaši agenti Managed File Transfer spuštěni v režimu klienta, příkazy, které budete muset vytvořit JKS (Java Keystore), jsou podrobně popsány v souboru “Stručná úvodní příručka pro klienty AMS with Java” na stránce 645.

Postup

1. Vytvořte certifikát podepsaný svým držitelem, abyste identifikovali uživatele `ftagent` , jak je podrobně popsáno v příslušné stručné úvodní příručce.
   Rozlišující název (DN) použijte takto:

   ```
   CN=ftagent, OU=MFT, O=<organisation>, L=<location>, ST=<state>, C=<country>
   ```

2. Vytvořte soubor `keystore.conf` , který identifikuje umístění úložiště klíčů a certifikát v něm, jak je podrobně popsáno v příslušné stručné úvodní příručce.

2. Konfigurace ochrany zpráv

Informace o této úloze

Měli byste definovat zásadu zabezpečení pro datovou frontu používanou produktem AGENT2pomocí příkazu **setmqspl** . V tomto scénáři se ke spuštění obou agentů použije stejný uživatel, a proto jsou rozlišující název podepsaného a příjemce stejné a odpovídají certifikátu, který jsme vygenerovali.

Postup

1. Vypněte agenty Managed File Transfer v rámci přípravy na ochranu pomocí příkazu **fteStopAgent** .
2. Vytvořte zásadu zabezpečení pro ochranu fronty SYSTEM.FTE.DATA.AGENT2 .

   ```
   setmqspl -m hubQM -p SYSTEM.FTE.DATA.AGENT2 -s SHA1 -a "CN=ftagent, OU=MFT,
   O=<organisation>, L=<location>, ST=<state>, C=<country>"
   -e AES128 -r "CN=ftagent, OU=MFT, O=<organisation>, L=<location>, ST=<state>, C=<country>"
   ```

3. Ujistěte se, že uživatel, který spustil proces Managed File Transfer Agent , má přístup k procházení fronty systémových zásad a vložení zpráv do fronty chyb.

   ```
   setmqaut -m hubQM -t queue -n SYSTEM.PROTECTION.POLICY.QUEUE -p ftagent +browse
   ```

   ```
   setmqaut -m hubQM -t queue -n SYSTEM.PROTECTION.ERROR.QUEUE -p ftagent +put
   ```

4. Restartujte agenty Managed File Transfer pomocí příkazu **fteStartAgent** .
5. Potvrďte, že se agenti úspěšně restartovali pomocí příkazu **fteListAgents** a ověřte, že jsou agenti ve stavu READY .

Výsledky

Nyní můžete odeslat přenosy z AGENT1 do AGENT2a obsah souboru bude bezpečně přenesen mezi dvěma agenty.

Advanced Message Security přehled instalace

Nainstalujte komponentu Advanced Message Security na různých platformách.

Procedura

- Instalovat Advanced Message Security na více platformách.
- Instalovat IBM MQ Advanced for z/OS.
- Instalovat IBM MQ Advanced for z/OS Value Unit Edition.

Související úlohy

OdinstalaceAdvanced Message Security

z/OS Auditování pro AMS on z/OS

Advanced Message Security (AMS) for z/OS poskytuje prostředky pro volitelné auditování operací aplikacemi ve frontách chráněných zásadami. Je-li tato volba povolena, záznamy auditu SMF (IBM System Management Facility) jsou generovány pro úspěch a selhání těchto operací ve frontách chráněných zásadami. Auditované operace zahrnují MQPUT, MQPUT1a MQGET.

Auditování je standardně zakázáno, avšak auditování můžete aktivovat nakonfigurováním _AMS_SMF_TYPE a _AMS_SMF_AUDIT v nakonfigurovaném jazykovém prostředí ® _CEE_ENVFILE pro adresní prostor AMS . Další informace naleznete v tématu Vytvoření procedur pro produkt Advanced Message Security. Proměnná _AMS_SMF_TYPE se používá k určení typu záznamu SMF a je číslem mezi 128 a 255. Typ záznamu SMF 180 je obvyklý, ale není povinný. Auditování je zakázáno zadáním hodnoty 0. Proměnná _AMS_SMF_AUDIT konfiguruje, zda jsou vytvořeny záznamy auditu pro operace, které jsou úspěšné, operace, které selhaly, nebo obojí. Volby monitorování lze také dynamicky měnit, když je AMS aktivní pomocí příkazů operátora. Další informace viz Provozní Advanced Message Security.

Záznam SMF je definován pomocí podtypů, přičemž podtyp 1 je obecná událost auditování. Záznam SMF obsahuje všechna data relevantní pro zpracovávaný požadavek.

Záznam SMF je mapován makrem CSQ0KSMF (všimněte si nuly v názvu makra), který je poskytován v cílové knihovně SCSQMACS. Pokud píšete programy pro redukci dat pro data SMF, můžete zahrnout toto mapovací makro, které vám pomůže při vývoji a přizpůsobení rutin SMF po zpracování.

V záznamech SMF vytvořených produktem Advanced Message Security for z/OSjsou data uspořádána do sekcí. Záznam se skládá z:

- standardní záhlaví SMF
- rozšíření záhlaví definované pomocí Advanced Message Security pro z/OS
- produktová sekce
- datovou sekci

Sekce produktu záznamu SMF je vždy přítomna v záznamech vytvořených Advanced Message Security pro z/OS. Datová sekce se liší v závislosti na podtypu. V současné době je definován jeden podtyp, a proto je použita jedna datová sekce.

Produkt SMF je popsán v příručce z/OS System Management Facilities (SA22-7630). Platné typy záznamů jsou popsány v členu SMFPRMxx datové sady PARMLIB vašeho systému. Další informace naleznete v dokumentaci SMF.

Advanced Message Security generátor sestav auditu (CSQ0USMF)

Advanced Message Security for z/OS poskytuje nástroj generátoru sestav auditu s názvem CSQ0USMF , který je poskytován v knihovně instalace SCSQAUTH. Ukázkový soubor JCL ke spuštění obslužného programu CSQ0USMF s názvem CSQ40RSM je uveden v instalační knihovně SCSQPROC.

Před spuštěním obslužného programu CSQ0USMF musí být záznamy SMF typu 180 vypsány z datových sad SMF systému do sekvenční datové sady. Tento skript JCL například vypíše záznamy SMF typu 180 z datové sady SMF a přenese je do cílové datové sady:

```
//IFAUDUMP EXEC PGM=IFASMFDP
//INDD1 DD DSN=SYSn.MANn.syst,DISP=SHR
//OUTDD1 DD DSN=your.target.dataset,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
INDD(INDD1,OPTIONS(DUMP))
OUTDD(OUTDD1,TYPE(180))
/*
```

Musíte ověřit skutečné názvy datových sad SMF, které vaše instalace používá. Cílová datová sada pro vypsaný záznam musí mít formát záznamu VBS a délku záznamu 32760.

Poznámka: Pokud se používají proudy protokolu SMF, musíte použít program IFASMFDL k výpisu proudu protokolu do sekvenční datové sady. Příklad použitého JCL viz Záznamy SMF typu zpracování 116 .

Cílovou datovou sadu lze poté použít jako vstup pro obslužný program CSQ0USMF k vytvoření sestavy auditu AMS . Příklad:

```
//STEP1 EXEC PGM=CSQ0USMF,
// PARM=('/ -SMFTYPE 180 -M qmgr')
//STEPLIB DD DSN=thlqual.SCSQANLE,DISP=SHR
//    DD DSN=thlqual.SCSQAUTH,DISP=SHR
//SMFIN DD DSN=your.target.dataset,DISP=SHR
//
```

Program CSQ0USMF přijímá dva volitelné parametry, které jsou uvedeny v souboru Tabulka 104 na stránce 657:

Tabulka 104. CSQ0USMF volitelné parametry

Parametr	Hodnota	Popis
SMFTYPE	nnn	Typ záznamu SMF použitelný pro sestavu auditu. Program CSQ0USMF používá při generování sestavy pouze záznamy SMF, které se shodují s hodnotou SMFTYPE. Pokud neuvedete SMFTYPE, použije se výchozí hodnota 180.
M	QMGR	Název správce front IBM MQ použitelný pro sestavu auditu. Pokud nezadáte parametr -M, bude sestava auditu obsahovat všechny záznamy auditu pro všechny správce front reprezentované v datové sadě SMFIN.

Použití úložišť klíčů a certifikátů s produktem AMS

K zajištění transparentní kryptografické ochrany pro aplikace IBM MQ používá produkt Advanced Message Security soubor úložiště klíčů, ve kterém jsou uloženy certifikáty veřejného klíče a soukromý klíč. V systému z/OSse místo souboru úložiště klíčů používá svazek klíčů SAF.

V produktu Advanced Message Securityjsou uživatelé a aplikace reprezentovány identitami infrastruktury veřejných klíčů (PKI). Tento typ identity se používá k podepisování a šifrování zpráv. Identita PKI je reprezentována polem **rozlišující název (DN)** subjektu v certifikátu, který je přidružen k podepsaným a šifrovaným zprávám. Aby mohl uživatel nebo aplikace šifrovat své zprávy, vyžadují přístup k souboru úložiště klíčů, kde jsou uloženy certifikáty a přidružené soukromé a veřejné klíče.

V systému AIX, Linux, and Windowsje umístění úložiště klíčů poskytnuto v konfiguračním souboru úložiště klíčů, což je standardně `keystore.conf` . Každý uživatel Advanced Message Security musí mít konfigurační soubor úložiště klíčů, který ukazuje na soubor úložiště klíčů. Produkt Advanced Message Security přijímá následující formát souborů úložiště klíčů: `.kdb`, `.jceks`, `.jks`.

Výchozí umístění souboru `keystore.conf` je:

- Linux IBM i AIX V systému IBM i, AIX and Linux: `$HOME/.mqs/keystore.conf`
- Windows V systému Windows: *%HOMEDRIVE%%HOMEPATH%*`\.mqs\keystore.conf`

Pokud používáte zadaný název souboru úložiště klíčů a umístění, měli byste jej zadat s proměnnou prostředí **MQS_KEYSTORE_CONF** , jak ukazuje následující příklad příkazů:

- Pro Java: `java -D`*`MQS_KEYSTORE_CONF=path/filename app_name`*

- Pro klienta a server C:
  - V systému AIX and Linux: `export MQS_KEYSTORE_CONF=path/filename`
  - V systému Windows: `set MQS_KEYSTORE_CONF=path\filename`

    Poznámka: Cesta v systému Windows může a měla by uvádět písmeno jednotky, pokud je k dispozici více než jedno písmeno jednotky.

Ochrana citlivých informací v souboru keystore.conf

Chcete-li získat přístup k citlivým informacím o souborech úložiště klíčů, jako jsou hesla, musíte zadat tokeny, aby mohl produkt IBM MQ Advanced Message Security (AMS) přistupovat k úložišti klíčů a podepisovat a šifrovat zprávy.

Citlivé informace obsažené v konfiguračním souboru úložiště klíčů byste měli chránit pomocí příkazu **runamscred** , který je součástí produktu AMS. Podrobnosti o tom, jak chránit konfigurační soubory, viz "Nastavení AMS ochrany heslem pro konfigurační soubory" na stránce 676 .

Při ochraně hesel byste měli používat vlastní, silný šifrovací klíč. Chcete-li přistupovat k heslům za běhu, musí být tento šifrovací klíč dodán do produktu AMS.

Existují dvě metody zadání umístění souboru šifrovacího klíče, které jsou prostřednictvím:

- Vlastnost konfigurace **amscred.keyfile** v souboru `keystore.conf`
- **MQS_AMSCRED_KEYFILE** proměnná prostředí

Pořadí priority je **MQS_AMSCRED_KEYFILE**, následované **amscred.keyfile**a pak výchozím klíčem.

Související pojmy

"Rozlišující názvy odesilatelů v souboru AMS" na stránce 686
Rozlišující názvy (DN) odesilatele identifikují uživatele, kteří jsou oprávněni umístit zprávy do fronty. Odesílatel používá svůj certifikát k podepsání zprávy před umístěním zprávy do fronty.

"Rozlišující názvy příjemců v souboru AMS" na stránce 687
Rozlišující názvy (DN) příjemců identifikují uživatele, kteří jsou autorizováni načítat zprávy z fronty.

Struktura konfiguračního souboru úložiště klíčů (keystore.conf) pro AMS

Konfigurační soubor úložiště klíčů (`keystore.conf`) ukazuje Advanced Message Security na umístění příslušného úložiště klíčů.

Každý z následujících typů konfiguračních souborů má předponu:

AMSCRED
Parametry, které se vztahují k systému ochrany heslem.

CMS
Systém správy certifikátů, položky konfigurace mají předponu: `cms.`

PKCS#11
Standard šifrování veřejného klíče #11, položky konfigurace mají předponu: `pkcs11.`

IBM i **PEM**
Formát Privacy Enhanced Mail, konfigurační položky mají předponu: `pem.`

JKS
Java KeyStore, položky konfigurace mají předponu: `jks.`

JCEKS
Java Šifrování KeyStore, položky konfigurace mají předponu: `jceks.`

z/OS MQ Adv. VUE **JCERACFKS**
Java Šifrování šifrování RACF svazek klíčů KeyStore, položky konfigurace mají předponu: `jceracfks`.

Důležité: V poli IBM MQ 9.0 jsou hodnoty `JCEKS.provider` a `JKS.provider` ignorovány. Poskytovatel Bouncy Castle se používá ve spojení s kterýmkoliv z ustanovení JCE/JCE, které dodává používané

prostředí JRE. Další informace viz “Podpora jiných prostředí JRE nežIBM s produktem AMS” na stránce 663.

Vzorové struktury pro úložiště klíčů:

CMS

```
cms.keystore = /dir/keystore_file
cms.certificate = certificate_label
```

PKCS#11

```
pkcs11.library = dir\cryptoki.dll
pkcs11.certificate = certificatelabel
pkcs11.token = tokenlabel
pkcs11.token_pin = tokenpin
pkcs11.secondary_keystore = dir\signers
V 9.3.0 pkcs11.encrypted = no
```

IBM i PEM

```
pem.private = /dir/keystore_file_private_key
pem.public = /dir/keystore_file_public_keys
pem.password = password
V 9.3.0 pem.encrypted = no
```

Java JKS

```
jks.keystore = dir/Keystore
jks.certificate = certificate_label
jks.encrypted = no
jks.keystore_pass = password
jks.key_pass = password
```

Java JCEKS

```
jceks.keystore = dir/Keystore
jceks.certificate = certificate_label
jceks.encrypted = no
jceks.keystore_pass = password
jceks.key_pass = password
```

Java JCERACFKS

```
jceracfks.keystore = safkeyring://user/keyring
jceracfks.certificate = certificate_label
```

Java PKCS#11

```
pkcs11.library = dir\cryptoki.dll
pkcs11.certificate = certificatelabel
pkcs11.token = tokenlabel
pkcs11.token_pin = tokenpin
pkcs11.secondary_keystore = dir\signers
pkcs11.secondary_keystore_pass = password
pkcs11.encrypted = no
```

Tabulka 105. Souhrn parametrů potřebných pro každý typ konfiguračního souboru						
		Typ konfiguračního souboru				
Parametry	**Povinné**	**Java (PKCS#11, JKS, JCEKS a JCERACFKS)**	**IBM i PEM**	**PKCS#11**	**CMS**	**AMSCRED**
keystore	✓	✓			✓	
IBM i private	✓		IBM i ✓			
IBM i public	✓		IBM i ✓			
IBM i password	✓		IBM i ✓			
library	✓	✓		✓		
certificate	✓	✓		✓	✓	
token	✓	✓		✓		
token_pin	✓	✓		✓		
secondary_keystore	✓	✓		✓		
secondary_keystore_password	✓	✓				
encrypted		✓	IBM i V 9.3.0 ✓	V 9.3.0 ✓		
keystore_pass	✓	✓				
key_pass		✓				
provider		✓				
keyfile						✓ Vy

Všimněte si, že můžete přidat komentáře pomocí symbolu # .

Parametry konfiguračního souboru jsou definovány takto:

keystore

Pouze konfigurace CMS a Java .

Cesta k souboru úložiště klíčů pro konfiguraci CMS, JKS a JCEKS.

z/OS MQ Adv. VUE Identifikátor URI pro svazek klíčů RACF pro konfiguraci JCERACFKS.

Důležité:

- Cesta k souboru úložiště klíčů nesmí obsahovat příponu souboru.
- z/OS MQ Adv. VUE Identifikátor URI pro svazek klíčů RACF musí být ve formátu:

  ```
  safkeyring://user/keyring
  ```

  kde:

  – *user* je ID uživatele, který vlastní svazek klíčů.

  – *keyring* je název svazku klíčů.

IBM i **private**
Pouze konfigurace PEM.

Název souboru, který obsahuje soukromý klíč a certifikát ve formátu PEM.

IBM i **public**
Pouze konfigurace PEM.

Název souboru, který obsahuje důvěryhodné veřejné certifikáty ve formátu PEM.

IBM i **password**
Pouze konfigurace PEM.

Heslo, které se používá k dešifrování zašifrovaného soukromého klíče.

V 9.3.0 Toto pole byste měli chránit pomocí nativního nástroje pro ochranu heslem AMS ; viz “Ochrana hesel” na stránce 662

library
PKCS#11 pouze.

Název cesty knihovny PKCS#11 .

certificate
Pouze konfigurace CMS, PKCS#11 a Java .

Popisek certifikátu

token
PKCS#11 pouze.

Popisek tokenu.

token_pin
PKCS#11 pouze.

Kód PIN pro odemknutí tokenu.

Pouze pro operace Java ; toto pole byste měli chránit pomocí nástroje pro ochranu hesla produktu Java AMS ; viz “Ochrana hesel” na stránce 662.

V 9.3.0 Pouze pro nativní operace; toto pole byste měli chránit pomocí nativního nástroje pro ochranu hesla AMS ; viz “Ochrana hesel” na stránce 662.

secondary_keystore
PKCS#11 pouze.

Název cesty k úložišti klíčů CMS , poskytnutý bez rozšíření `.kdb` , které obsahuje kotevní certifikáty (kořenové certifikáty) požadované certifikáty uloženými v tokenu PKCS #11 . Sekundární úložiště klíčů může také obsahovat certifikáty, které jsou v řetězci důvěryhodnosti přechodné, a také certifikáty příjemců, které jsou definovány v zásadách zabezpečení ochrany osobních údajů. Toto úložiště klíčů CMS musí být doprovázeno souborem pro dočasné ukládání, který musí být umístěn ve stejném adresáři jako sekundární úložiště klíčů.

Pro prostředí Java je vyžadováno úložiště klíčů JKS a musíte poskytnout **secondary_keystore_password**.

secondary_keystore_password
Pouze Java PKCS#11 .

Heslo pro úložiště klíčů JKS poskytnuté prostřednictvím vlastnosti `secondary_keystore` . Toto pole byste měli chránit pomocí nástroje pro ochranu hesla produktu Java AMS ; viz “Ochrana hesel” na stránce 662.

encrypted
Java V 9.3.0 a z IBM MQ 9.3.0pouze PKCS#11 a IBM i PEM .

Stav hesla.

keystore_pass
Pouze konfigurace Java .

Heslo pro soubor úložiště klíčů.

Pouze pro operace Java . Toto pole byste měli chránit pomocí nástroje pro ochranu hesla produktu Java AMS ; viz “Ochrana hesel” na stránce 662.

key_pass
Pouze konfigurace Java .

Heslo pro soukromý klíč uživatele.

Pouze pro operace Java ; toto pole byste měli chránit pomocí nástroje pro ochranu hesla produktu Java AMS ; viz “Ochrana hesel” na stránce 662.

keyfile
Poskytuje umístění počátečního klíče, který se má použít při ochraně nebo dešifrování hesel obsažených v tomto konfiguračním souboru; viz “Ochrana hesel” na stránce 662

provider
Pouze konfigurace Java .

Poskytovatel zabezpečení Java , který implementuje šifrovací algoritmy požadované certifikátem úložiště klíčů.

Důležité: Informace uložené v úložišti klíčů jsou klíčové pro zabezpečený tok dat odesílaných pomocí produktu IBM MQ. Administrátoři zabezpečení musí věnovat zvláštní pozornost při přiřazování oprávnění k souborům těmto souborům.

Ochrana hesel

Měli byste chránit hesla a další citlivé informace obsažené v souboru `keystore.conf` . Další informace naleznete v tématu **runamscred**.

Příklad souboru `keystore.conf` :

```
# Native AMS application configuration
cms.keystore = c:\Documents and Settings\Alice\AliceKeystore
cms.certificate = AliceCert

# Java AMS application configuration
jceks.keystore = c:/Documents and Settings/Alice/AliceKeystore
jceks.certificate = AliceCert
jceks.encrypted = no
jceks.keystore_pass = passw0rd
jceks.key_pass = passw0rd
jceks.provider = IBMJCE
```

Související úlohy

“Nastavení AMS ochrany heslem pro konfigurační soubory” na stránce 676
Ukládání hesel úložiště klíčů a soukromých klíčů jako prostého textu představuje bezpečnostní riziko, takže produkt Advanced Message Security poskytuje nástroj, který může tato hesla použít pomocí klíče uživatele.

Podpora jiných prostředí JRE nežIBM s produktem AMS

Operace IBM MQ classes for Java a IBM MQ classes for JMS support Advanced Message Security při spuštění s jinými nežIBM JRE.

Advanced Message Security (AMS) implementuje syntaxi šifrovacích zpráv (CMS). Syntaxe CMS se používá k digitálnímu podpisu, výběru, ověření nebo šifrování libovolného obsahu zprávy.

V operačním systému IBM MQ 9.0podpora Advanced Message Security v systémech IBM MQ classes for Java a IBM MQ classes for JMS používá k podpoře systému CMSbalíky Bouncy Castle s otevřeným zdrojem. To znamená, že tyto třídy mohou podporovat operaci Advanced Message Security při spuštění jiných prostředí JRE nežIBM .

Před IBM MQ 9.0nebylo prostředí Advanced Message Security podporováno v jiných nežIBM JRE v klientech Java . Podpora Advanced Message Security v systémech IBM MQ classes for Java a IBM MQ classes for JMS závisí na podpoře CMS specificky poskytované implementací IBM rozšíření JCE (Java Cryptography Extensions). Kvůli tomuto omezení byla funkčnost k dispozici pouze při použití prostředí Java runtime environment (JRE), které obsahovalo poskytovatele JCE Java .

Umístění a číslování verzí pro soubory JAR zámku Bouncy

Soubory JAR Bouncy Castle, které jsou potřebné pro podporu jiných prostředí JRE nežIBM , jsou zahrnuty jako součást instalačního balíku IBM MQ classes for Java a IBM MQ classes for JMS .

Použité soubory JAR Bouncy Castle jsou následující soubory:

Soubor JAR poskytovatele, který je zásadní pro operace Bouncy Castle.

V 9.3.5 Pro Continuous Delivery z IBM MQ 9.3.5se tento soubor JAR nazývá `bcprov-jdk18on.jar`.

LTS Pro Long Term Support a Continuous Delivery před IBM MQ 9.3.5se tento soubor JAR nazývá `bcprov-jdk15to18.jar`.

Soubor JAR "PKIX", který obsahuje podporu operací CMS používaných produktem Advanced Message Security.

V 9.3.5 Pro Continuous Delivery z IBM MQ 9.3.5se tento soubor JAR nazývá `bcpkix-jdk18on.jar`.

LTS Pro Long Term Support a Continuous Delivery před IBM MQ 9.3.5se tento soubor JAR nazývá `bcpkix-jdk15to18.jar`.

Soubor JAR "util", který obsahuje třídy používané ostatními soubory JAR Bouncy Castle.

V 9.3.5 Pro Continuous Delivery z IBM MQ 9.3.5se tento soubor JAR nazývá `bcutil-jdk18on.jar`.

LTS Pro Long Term Support a Continuous Delivery před IBM MQ 9.3.5se tento soubor JAR nazývá `bcutil-jdk15to18.jar`.

Závislosti

Třídy IBM MQ 9.1 a novější byly testovány s prostředím JRE systému IBM a Oracle . Rovněž je pravděpodobné, že budou úspěšně spuštěny v libovolném prostředí J2SE-compliant JRE. Měli byste si však uvědomit následující závislosti:

- V konfiguraci produktu Advanced Message Security nejsou žádné změny.
- Třídy Bouncy Castle se používají pouze pro operace CMS . Všechny ostatní operace související se zabezpečením, například přístup k úložišti klíčů, skutečné šifrování dat a výpočet kontrolních součtů podpisu, používají funkčnost, kterou poskytuje prostředí JRE.

  Důležité: Z tohoto důvodu musí použité prostředí JRE obsahovat implementaci poskytovatele JCE.
- Chcete-li použít některé *silné* šifrovací algoritmy, možná budete muset nainstalovat *neomezené* soubory zásad pro implementaci JCE prostředí JRE.

Další podrobnosti naleznete v dokumentaci k prostředí JRE.

- Pokud jste povolili zabezpečení Java :
  - Přidejte `java.security.SecurityPermissioninsertProvider.BC` do aplikace, aby bylo možné použít třídy Bouncy Castle jako poskytovatele zabezpečení.
  - Udělte oprávnění `java.security.AllPermission` pro soubory JAR zámku Bouncy.

    V 9.3.5 Pro Continuous Delivery z IBM MQ 9.3.5jsou tyto soubory:

    mq_install_dir`/java/lib/bcutil-jdk18on.jar`
    mq_install_dir`/java/lib/bcpkix-jdk18on.jar`
    mq_install_dir`/java/lib/bcprov-jdk18on.jar`

    LTS Pro Long Term Support a Continuous Delivery před IBM MQ 9.3.5

    mq_install_dir`/java/lib/bcutil-jdk15to18.jar`
    mq_install_dir`/java/lib/bcpkix-jdk15to18.jar`
    mq_install_dir`/java/lib/bcprov-jdk15to18.jar`

Související pojmy
Co je instalováno pro třídy IBM MQ pro JMS
Co je instalováno pro třídy IBM MQ pro Java

Multi Zachycení agenta MCA (Message Channel Agent) a AMS

Zachycení MCA umožňuje správci front spuštěnému v adresáři IBM MQ selektivně povolit použití zásad pro kanály připojení serveru.

Zachycení MCA umožňuje klientům, kteří zůstávají mimo produkt AMS , aby byli stále připojeni ke správci front a jejich zprávy byly šifrovány a dešifrovány.

Zachycení MCA má poskytovat AMS schopnost, když AMS nemůže být povoleno na klientovi. Všimněte si, že použití zachycení MCA a klienta s povoleným produktem AMSvede k dvojité ochraně zpráv, což může být problematické pro příjem aplikací. Další informace viz “Zakázání Advanced Message Security na klientovi” na stránce 667.

Poznámka: Zachytávače MCA nejsou podporovány pro kanály AMQP nebo MQTT.

Konfigurační soubor úložiště klíčů

Standardně je konfigurační soubor úložiště klíčů pro zachycení MCA `keystore.conf` a je umístěn v adresáři `.mqs` v cestě k adresáři HOME uživatele, který spustil správce front nebo modul listener. Úložiště klíčů lze konfigurovat také pomocí proměnné prostředí MQS_KEYSTORE_CONF. Další informace o konfiguraci úložiště klíčů AMS viz “Použití úložišť klíčů a certifikátů s produktem AMS” na stránce 657.

Chcete-li povolit zachycení MCA, musíte zadat název kanálu, který chcete použít v konfiguračním souboru úložiště klíčů. Pro zachycení MCA lze použít pouze typ úložiště klíčů cms.

Příklad nastavení zachycení MCA viz “Příklad zachycení MCA pro AMS” na stránce 665 .

Upozornění: Musíte dokončit ověření a šifrování klienta na vybraných kanálech, například pomocí SSL a SSLPEER nebo CHLAUTH TYPE (SSLPEERMAP), abyste se ujistili, že se mohou připojit a používat tuto schopnost pouze autorizovaní klienti.

IBM i

Pokud váš podnik používá produkt IBM ia vy jste pro podepsání certifikátu vybrali komerční certifikační autoritu (CA), produkt Digital Certificate Manager vytvoří žádost o certifikát ve formátu PEM (Privacy-Enhanced Mail). Požadavek musíte předat vybrané certifikační autoritě.

Chcete-li tak učinit, musíte pomocí následujícího příkazu vybrat správný certifikát pro kanál určený v souboru `channelname`:

```
pem.certificate.channel.channelname
```

Příklad zachycení MCA pro AMS

Vzorová úloha týkající se nastavení zachycení modulu MCA AMS .

Než začnete

Upozornění: Musíte dokončit ověření a šifrování klienta na vybraných kanálech, například pomocí SSL a SSLPEER nebo CHLAUTH TYPE (SSLPEERMAP), abyste se ujistili, že se mohou připojit a používat tuto schopnost pouze autorizovaní klienti.

Pokud váš podnik používá produkt IBM ia vy jste pro podepsání certifikátu vybrali komerční certifikační autoritu (CA), produkt Digital Certificate Manager vytvoří žádost o certifikát ve formátu PEM (Privacy-Enhanced Mail). Požadavek musíte předat vybrané certifikační autoritě.

Informace o této úloze

Tato úloha vás provede procesem nastavení systému tak, aby používal zachycení MCA, a poté ověří nastavení.

Poznámka: IBM MQzahrnuje zachytávače AMS a dynamicky je povoluje v běhových prostředích klienta a serveru MQ .

Upozornění:

- Nahraďte `userID` v kódu svým ID uživatele.
- Následující postup nefunguje podle očekávání v produktu IBM MQ , pokud není zachycení AMS na klientovi deaktivováno.

Postup

1. Vytvořte databázi klíčů a certifikáty pomocí následujících příkazů pro vytvoření skriptu shellu.

   Také změňte **INSTLOC** a **KEYSTORELOC** nebo spusťte požadované příkazy. Všimněte si, že možná nebudete muset vytvořit certifikát pro bob.

```
INSTLOC=/opt/mqm
KEYSTORELOC=/home/userID/var/mqm
mkdir -p $KEYSTORELOC
chmod -R 777 $KEYSTORELOC
chown -R mqm:mqm $KEYSTORELOC
export PATH=$PATH:$INSTLOC/gskit8/bin
echo "PATH = $PATH"
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$INSTLOC/gskit8/lib64

runmqakm -keydb -create -db $KEYSTORELOC/alicekey.kdb -pw passw0rd -stash
runmqakm -keydb -create -db $KEYSTORELOC/bobkey.kdb -pw passw0rd -stash
runmqakm -cert -create -db $KEYSTORELOC/alicekey.kdb -pw passw0rd \
-label alice_cert -dn "cn=alice,O=IBM,c=IN" -default_cert yes
runmqakm -cert -create -db $KEYSTORELOC/bobkey.kdb -pw passw0rd \
-label bob_cert  -dn "cn=bob,O=IBM,c=IN"  -default_cert yes
```

2. Sdílejte certifikáty mezi těmito dvěma databázemi klíčů, aby každý uživatel mohl úspěšně identifikovat druhého.

   Je důležité, abyste použili metodu popsanou pro sdílení certifikátů v *Stručné úvodní příručce*pro platformu, kterou váš podnik používá:

   Windows
   Úloha 5 Sdílení certifikátů

   AIX and Linux
   Úloha 5 Sdílení certifikátů

Java klienti
Úloha 5 Sdílení certifikátů

3. Vytvořte soubor `keystore.conf` s následující konfigurací: `Keystore.conf location: /home/userID/ssl/ams1/`

```
cms.keystore = /home/userID/ssl/ams1/alicekey
cms.certificate.channel.SYSTEM.DEF.SVRCONN = alice_cert
```

Upozornění:

a. Úložiště klíčů musí být v systému, kde je správce front.

b. Chcete-li povolit intervenci MCA, musíte zadat specifický kanál pro produkt `cms.certificate` a poté správce front provede operace AMS v aplikacích, které se prostřednictvím tohoto kanálu připojují k frontám se sadou zásad.

4. Vytvořit a spustit správce front AMSQMGR1
5. Definujte modul listener TCP pomocí dostupného čísla portu pod řízením QMGR.

   Příklad:

```
DEFINE LISTENER(MY.LISTENER) TRPTYPE(TCP) PORT(14567) CONTROL(QMGR)
```

6. Spusťte modul listener a ověřte, že byl správně spuštěn.

   Příklad:

```
START  LISTENER(MY.LISTENER)
DISPLAY LSSTATUS(MY.LISTENER) PORT
```

7. Zastavte správce front.
8. Nastavte úložiště klíčů:

```
export MQS_KEYSTORE_CONF=/home/userID/ssl/ams1/keystore.conf
```

9. Spusťte správce front ve stejném shellu, aby byla pro správce front k dispozici proměnná prostředí MQS_KEYSTORE_CONF.
10. Nastavte zásadu zabezpečení a ověřte:

```
setmqspl -m AMSQMGR1 -s SHA256 -e AES256 -p TESTQ -a "CN=alice,O=IBM,C=IN" \
-r "CN=alice,O=IBM,C=IN"
dspmqspl -m AMSQMGR1
```

    Další informace viz setmqspl a dspmqspl .

11. Nastavte proměnnou prostředí *MQSERVER* :

```
export MQSERVER='SYSTEM.DEF.SVRCONN/TCP/127.0.0.1(14567)'
```

12. Odeberte zásadu zabezpečení a ověřte výsledek:

```
setmqspl -m AMSQMGR1 -p TESTQ -remove
dspmqspl -m AMSQMGR1
```

13. Procházejte frontu z instalace produktu IBM MQ 9.3 :

```
/opt/mq93/samp/bin/amqsbcg TESTQ AMSQMGR1
```

    Výstup procházení zobrazuje zprávy v zašifrovaném formátu.

14. Nastavte zásadu zabezpečení a ověřte výsledek:

```
setmqspl -m AMSQMGR1 -s SHA256 -e AES256 -p TESTQ -a "CN=alice,O=IBM,C=IN"
-r "CN=alice,O=IBM,C=IN"
dspmqspl -m AMSQMGR1
```

15. Spusťte příkaz **amqsgetc** z instalace produktu IBM MQ 9.3 :

```
/opt/mqm/samp/bin/amqsgetc TESTQ TESTQMGR
```

Související pojmy

“Struktura konfiguračního souboru úložiště klíčů (keystore.conf) pro AMS” na stránce 658
Konfigurační soubor úložiště klíčů (`keystore.conf`) ukazuje Advanced Message Security na umístění příslušného úložiště klíčů.

Související odkazy

“Známá omezení AMS” na stránce 617
Existuje řada voleb IBM MQ , které buď nejsou podporovány, nebo mají omezení pro Advanced Message Security.

Zakázání Advanced Message Security na klientovi

Pokud používáte klienta IBM MQ pro připojení ke správci front ze starší verze produktu a byla ohlášena chyba `2085 (MQRC_UNKNOWN_OBJECT_NAME)` , musíte produkt IBM MQ Advanced Message Security (AMS) zakázat.

Informace o této úloze

Funkce IBM MQ Advanced Message Security (AMS) je automaticky povolena v klientu IBM MQ , a proto se klient standardně pokouší zkontrolovat zásady zabezpečení pro objekty ve správci front.

Pokud je tato chyba ohlášena a pokoušíte se připojit ke správci front z dřívější verze produktu, můžete produkt AMS zakázat následujícím způsobem:

- Pro klienty systému Java jedním z následujících způsobů:
  - Nastavením proměnné prostředí **AMQ_DISABLE_CLIENT_AMS**.
  - Nastavením Java systémové vlastnosti com.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS.
  - Pomocí vlastnosti **DisableClientAMS** v sekci Zabezpečení v souboru `mqclient.ini` .
- Pro klienty C nastavením proměnné prostředí **MQS_DISABLE_ALL_INTERCEPT**.

Poznámka: Pro klienty jazyka C nelze použít proměnnou prostředí **AMQ_DISABLE_CLIENT_AMS** . Místo toho musíte použít proměnnou prostředí **MQS_DISABLE_ALL_INTERCEPT** .

Procedura

- Chcete-li zakázat produkt AMS na klientovi, použijte jednu z následujících voleb:

  proměnná prostředí AMQ_DISABLE_CLIENT_AMS
  Tuto proměnnou je třeba nastavit v následujících případech:
  - Pokud používáte jiné prostředí Java runtime environment (JRE) než IBM Java runtime environment (JRE)
  - Pokud používáte klienta IBM MQ IBM MQ classes for JMS nebo IBM MQ classes for Java .

  Vytvořte proměnnou prostředí **AMQ_DISABLE_CLIENT_AMS** a nastavte ji na hodnotu TRUE v prostředí, kde je aplikace spuštěna. Příklad:

  ```
  export AMQ_DISABLE_CLIENT_AMS=TRUE
  ```

  Java systémová vlastnost com.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS
  U klientů IBM MQ classes for JMS a IBM MQ classes for Java můžete nastavit systémovou vlastnost Java com.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS na hodnotu TRUE pro aplikaci Java .

  Například můžete nastavit systémovou vlastnost Java jako volbu `-D` při vyvolání příkazu Java :

  ```
  V 9.3.0 JM 3.0 V 9.3.0 java -Dcom.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS=TRUE
  -cp <MQ_INSTALLATION_PATH>/java/lib/com.ibm.mq.jakarta.client.jar
  my.java.applicationClass
  ```

```
JMS 2.0 java -Dcom.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS=TRUE -cp <MQ_INSTALLATION_PATH>/
java/lib/com.ibm.mq.allclient.jar  my.java.applicationClass
```

Alternativně můžete uvést systémovou vlastnost Java v JMS konfiguračním souboru `jms.config`, pokud aplikace používá tento soubor.

proměnná prostředí MQS_DISABLE_ALL_INTERCEPT

Tuto proměnnou prostředí musíte nastavit, pokud používáte IBM MQ s nativními klienty a musíte zakázat AMS na klientovi.

Vytvořte proměnnou prostředí **MQS_DISABLE_ALL_INTERCEPT** a nastavte ji na hodnotu TRUE v prostředí, kde je spuštěn klient. Příklad:

```
export MQS_DISABLE_ALL_INTERCEPT =TRUE
```

Proměnnou prostředí **MQS_DISABLE_ALL_INTERCEPT** můžete použít pouze pro klienty jazyka C. Pro klienty systému Java musíte místo toho použít proměnnou prostředí **AMQ_DISABLE_CLIENT_AMS** .

Vlastnost DisableClientAMS v souboru mqclient.ini

Tuto volbu můžete použít pro klienty IBM MQ classes for JMS a IBM MQ classes for Java a pro klienty C.

Přidejte název vlastnosti DisableClientAMS pod sekci **Security** souboru `mqclient.ini` , jak ukazuje následující příklad:

```
Security:
DisableClientAMS=Yes
```

Můžete také povolit AMS , jak ukazuje následující příklad:

```
Security:
DisableClientAMS=No
```

Jak pokračovat dále

Další informace o problémech s otevíráním chráněných front systému AMS naleznete v tématu Problémy s otevíráním chráněných front při použití produktu AMS s produktem JMS.

Související pojmy

“Zachycení agenta MCA (Message Channel Agent) a AMS” na stránce 664

Zachycení MCA umožňuje správci front spuštěnému v adresáři IBM MQ selektivně povolit použití zásad pro kanály připojení serveru.

Související úlohy

IBM MQ MQI client konfigurační soubor, `mqclient.ini`

Související odkazy

Konfigurační soubor IBM MQ classes for JMS

Požadavky na certifikáty pro AMS

Certifikáty musí mít veřejný klíč RSA, aby mohly být použity s produktem Advanced Message Security.

Další informace o různých typech veřejných klíčů a o tom, jak je vytvořit, viz “Digitální certifikáty a kompatibilita CipherSpec v produktu IBM MQ” na stránce 46.

Rozšíření použití klíče

Rozšíření použití klíče dále omezují způsob použití certifikátu.

V systému Advanced Message Securitymusí být použití klíče certifikátů X.509 v3 nastaveno v souladu se specifikací RFC 5280.

Pro zajištění kvality integrity ochrany, jsou-li nastavena rozšíření použití klíče certifikátu, musí tato sada obsahovat alespoň jednu z těchto dvou možností:

- **nonRepudiation**
- **digitalSignature**

Pro zajištění kvality ochrany soukromí platí, že pokud jsou nastavena rozšíření použití klíče certifikátu, musí tato sada obsahovat:

- **keyEncipherment**

V případě, že jsou nastavena rozšíření použití klíče certifikátu pro zachování důvěrnosti, musí tato sada obsahovat:

- **dataEncipherment**

Rozšířené použití klíče dále upřesňuje rozšíření použití klíče. Pro všechny kvality ochrany platí, že pokud je nastaveno rozšířené použití klíče certifikátu, musí sada obsahovat:

- **emailProtection**

Související pojmy

"Kvalita ochrany v AMS" na stránce 689
Zásady ochrany dat Advanced Message Security znamenají kvalitu ochrany (QOP).

Metody ověření platnosti certifikátu v souboru AMS

Produkt Advanced Message Security můžete použít ke zjištění a zamítnutí odvolaných certifikátů, aby zprávy ve frontách nebyly chráněny pomocí certifikátů, které nesplňují standardy zabezpečení.

Produkt AMS umožňuje ověřit platnost certifikátu pomocí protokolu OCSP (Online Certificate Status Protocol) nebo seznamu odvolaných certifikátů (CRL).

Produkt AMS lze konfigurovat buď pro kontrolu OCSP, nebo CRL, nebo pro obojí. Jsou-li povoleny obě metody, produkt AMS z důvodů výkonu nejprve použije protokol OCSP pro stav odvolání. Není-li stav odvolání certifikátu po kontrole OCSP určen, produkt AMS použije kontrolu CRL.

Všimněte si, že kontrola OCSP i CRL je standardně povolena.

Související pojmy

"Protokol OCSP (Online Certificate Status Protocol) v adresáři AMS" na stránce 669
Protokol OCSP (Online Certificate Status Protocol) určuje, zda byl certifikát odvolán, a proto pomáhá určit, zda může být certifikát důvěryhodný. Protokol OCSP je standardně povolen.

"Seznamy odvolaných certifikátů (CRL) v souboru AMS" na stránce 671
Seznamy CRL obsahují seznam certifikátů, které byly označeny certifikační autoritou (CA) jako nedůvěryhodné z různých důvodů, například soukromý klíč byl ztracen nebo ohrožen.

Protokol OCSP (Online Certificate Status Protocol) v adresáři AMS

Protokol OCSP (Online Certificate Status Protocol) určuje, zda byl certifikát odvolán, a proto pomáhá určit, zda může být certifikát důvěryhodný. Protokol OCSP je standardně povolen.

Protokol OCSP není v systémech IBM i podporován.

Povolení vracení protokolu OCSP v nativních zachytávačích Advanced Message Security
Kontrola protokolu OCSP (Online Certificate Status Protocol) v produktu Advanced Message Security je standardně povolena na základě informací v používaných certifikátech.

Postup

Přidejte do konfiguračního souboru úložiště klíčů tyto volby:

Poznámka: Všechny sekce OCSP jsou volitelné a lze je zadat nezávisle.

Volba	Popis
`ocsp.enable=off`	Povolte kontrolu OCSP, pokud má kontrolovaný certifikát rozšíření AIA (Authority Info Access) s přístupovou metodou PKIX_AD_OCSP obsahující identifikátor URI, kde je umístěn odpovídací modul OCSP. Možné hodnoty: on nebo `off`.
`ocsp.url=`*`responder_URL`*	Adresa URL odpovídacího modulu OCSP. Pokud je tato volba vynechána, je kontrola OCSP mimo AIA zakázána.
`ocsp.http.proxy.host=`*`OCSP_proxy`*	Adresa URL serveru proxy OCSP. Je-li tato volba vynechána, server proxy se nepoužije pro kontroly online certifikátů jiných než AIA.
`ocsp.http.proxy.port=`*`port_number`*	Číslo portu serveru proxy OCSP. Pokud je tato volba vynechána, použije se výchozí port 8080.
`ocsp.nonce.generation=on/off`	Generovat nonce (náhodně generované číslo) při dotazování OCSP. Výchozí hodnota je `off`.
`ocsp.nonce.check=on/off`	Kontrolovat nonce (náhodně generované číslo) po přijetí odezvy z OCSP. Výchozí hodnota je `off`.
`ocsp.nonce.size=8`	Velikost nonce (náhodně generovaného čísla) v bajtech.
`ocsp.http.get=on/off`	Určete operaci HTTP GET jako metodu svého požadavku. Je-li pro tuto volbu nastavena hodnota `off`, použije se metoda HTTP POST. Výchozí hodnota je `off`.
`ocsp.max_response_size=20480`	Maximální velikost odezvy odpovídacího modulu OCSP v bajtech.
`ocsp.cache_size=100`	Povolte interní mezipaměť odezvy OCSP a nastavte mezní hodnotu počtu položek mezipaměti.
`ocsp.timeout=30`	Doba čekání na odezvu serveru v sekundách. Po uplynutí této doby dojde k vypršení časového limitu Advanced Message Security.
`ocsp.unknown=ACCEPT`	Definuje chování v případě, že server OCSP není dosažitelný během časového limitu. Možné hodnoty jsou: • `ACCEPT` Umožňuje certifikát • `WARN` Umožňuje certifikát a protokoluje varování • `REJECT` Zabraňuje použití certifikátu a protokoluje chybu

Povolení vracení protokolu OCSP Java v AMS
Chcete-li povolit kontrolu protokolu OCSP pro Java v souboru Advanced Message Security, upravte soubor `java.security` nebo konfigurační soubor úložiště klíčů.

Informace o této úloze

Existují dva způsoby, jak povolit kontrolu OCSP v produktu Advanced Message Security:

Použití java.security
Zkontrolujte, zda váš certifikát obsahuje rozšíření certifikátu AIA (Authority Information Access).

Postup

1. Není-li oblast AIA nastavena nebo chcete-li přepsat svůj certifikát, upravte soubor `$JAVA_HOME/lib/security/java.security` s následujícími vlastnostmi:

   ```
   ocsp.responderURL=http://url.to.responder:port
   ocsp.responderCertSubjectName=CN=Example CA,O=IBM,C=US
   ```

   a povolte kontrolu OCSP úpravou souboru `$JAVA_HOME/lib/security/java.security` na následujícím řádku:

   ```
   ocsp.enable=true
   ```

2. Je-li nastavena oblast AIA, povolte kontrolu OCSP úpravou souboru `$JAVA_HOME/lib/security/java.security` na následujícím řádku:

   ```
   ocsp.enable=true
   ```

Jak pokračovat dále

Pokud používáte produkt Java Security Manager, dokončete také konfiguraci, přidejte následující Java oprávnění k `lib/security/java.policy`

```
permission java.security.SecurityPermission "getProperty.ocsp.enable";
```

Použití souboru keystore.conf

Postup

Do konfiguračního souboru přidejte následující atribut:

```
ocsp.enable=true
```

Důležité: Nastavení tohoto atributu v konfiguračním souboru přepíše nastavení java.security .

Jak pokračovat dále

Chcete-li dokončit konfiguraci, přidejte do souboru `lib/security/java.policy`následující Java oprávnění:

```
permission java.security.SecurityPermission "getProperty.ocsp.enable";
permission java.security.SecurityPermission "setProperty.ocsp.enable";
```

Seznamy odvolaných certifikátů (CRL) v souboru AMS

Seznamy CRL obsahují seznam certifikátů, které byly označeny certifikační autoritou (CA) jako nedůvěryhodné z různých důvodů, například soukromý klíč byl ztracen nebo ohrožen.

Chcete-li ověřit certifikáty, produkt Advanced Message Security vytvoří řetěz certifikátů, který se skládá z certifikátu podepsaného a řetězu certifikátů certifikační autority (CA) až po kotvu důvěryhodnosti. Kotva důvěryhodnosti je soubor důvěryhodného úložiště klíčů, který obsahuje důvěryhodný certifikát nebo důvěryhodný kořenový certifikát, který se používá k deklarování důvěryhodnosti certifikátu. Produkt

AMS ověří cestu k certifikátu pomocí ověřovacího algoritmu PKIX. Když je řetěz vytvořen a ověřen, produkt AMS dokončí ověření certifikátu, které zahrnuje ověření vydání a data vypršení platnosti každého certifikátu v řetězu oproti aktuálnímu datu, a zkontroluje, zda je rozšíření použití klíče přítomno v certifikátu koncové entity. Pokud je rozšíření připojeno k certifikátu, produkt AMS ověří, zda jsou také nastaveny položky **digitalSignature** nebo **nonRepudiation** . Pokud nejsou, je hlášen a protokolován soubor MQRC_SECURITY_ERROR . Dále produkt AMS stáhne seznamy CRL ze souborů nebo z LDAP v závislosti na tom, jaké hodnoty byly uvedeny v konfiguračním souboru. AMSpodporuje pouze seznamy CRL, které jsou zakódovány ve formátu DER. Pokud není v konfiguračním souboru úložiště klíčů nalezena žádná konfigurace související se seznamem CRL, produkt AMS neprovede žádnou kontrolu platnosti seznamu CRL. Pro každý certifikát certifikační autority se produkt AMS dotazuje LDAP na seznamy CRL pomocí rozlišujících názvů certifikační autority, aby vyhledal seznam CRL. V dotazu LDAP jsou zahrnuty následující atributy:

```
certificateRevocationList,
certificateRevocationList;binary,
authorityRevocationList,
authorityRevocationList;binary
deltaRevocationList
deltaRevocationList;binary,
```

Poznámka: Parametr `deltaRevocationList` je podporován pouze v případě, že je určen jako distribuční body.

Povolení podpory ověřování certifikátů a seznamu odvolaných certifikátů v nativních zachytávačích
Konfigurační soubor úložiště klíčů musíte upravit tak, aby produkt Advanced Message Security mohl stahovat soubory CLR ze serveru LDAP (Lightweight Directory Access Protocol).

Informace o této úloze

IBM i Povolení podpory ověřování certifikátů a seznamu odvolaných certifikátů v nativních zachytávačích není pro systém Advanced Message Security on IBM ipodporováno.

Postup

Do konfiguračního souboru přidejte následující volby:

Poznámka: Všechny sekce CRL jsou volitelné a lze je zadat nezávisle.

Volba	Popis
`crl.ldap.host=`*`host_name`*	Název hostitele serveru LDAP.
`crl.ldap.port=`*`port_number`*	Číslo portu serveru LDAP. Můžete uvést až 11 serverů. K zajištění transparentního překonání selhání v případě selhání připojení LDAP se používá více hostitelů LDAP. Očekává se, že všechny servery LDAP jsou repliky a obsahují stejná data. Když se zachytávač AMS Java úspěšně připojí k serveru LDAP, nepokusí se stáhnout seznamy CRL ze zbývajících poskytnutých serverů.
`crl.cdp=off`	Pomocí této volby můžete v certifikátech zaškrtnout nebo použít rozšíření CRLDistributionPoints .
`crl.ldap.version=3`	Číslo verze protokolu LDAP. Možné hodnoty: 2 nebo 3.

Volba	Popis
`crl.ldap.user=cn=`*username*	Přihlaste se k serveru LDAP. Není-li tato hodnota uvedena, atributy CRL v LDAP musí být čitelné pro všechny
`crl.ldap.pass=`*password*	Heslo pro server LDAP.
V 9.3.0 `crl.ldap.encrypted=`*no/yes*	Zda je soubor `clr.ldap.pass` šifrovaný, či nikoli. Další informace viz Ochrana hesel v konfiguračních souborech AMS .
`crl.ldap.cache_lifetime=0`	Doba životnosti mezipaměti LDAP v sekundách. Možné hodnoty: 0-86400.
`crl.ldap.cache_size=50`	Velikost mezipaměti LDAP. Tuto volbu lze zadat pouze v případě, že hodnota `crl.ldap.cache_lifetime` je větší než `0`.
`crl.http.proxy.host=some.host.com`	Port serveru proxy HTTP pro načtení CRL CDP.
`crl.http.proxy.port=8080`	Číslo portu serveru proxy HTTP.
`crl.http.max_response_size=204800`	Maximální velikost seznamu CRL v bajtech, kterou lze načíst ze serveru HTTP, který je přijat produktem IBM Global Security Kit (GSKit).
`crl.http.timeout=30`	Doba čekání na odezvu serveru v sekundách, po které AMS vyprší časový limit.
`crl.http.cache_size=0`	Velikost mezipaměti HTTP, v bajtech.
`crl.unknown=ACCEPT`	Definuje chování, když nelze dosáhnout serveru CRL během časového limitu. Možné hodnoty jsou: • `ACCEPT` Umožňuje certifikát • `WARN` Umožňuje certifikát a protokoluje varování • `REJECT` Zabraňuje použití certifikátu a protokoluje chybu

Povolení podpory seznamu odvolaných certifikátů v Java v AMS
Chcete-li povolit podporu seznamů CRL v produktu Advanced Message Security, musíte upravit konfigurační soubor úložiště klíčů tak, aby AMS mohl stahovat seznamy CRL ze serveru LDAP (Lightweight Directory Access Protocol) a konfigurovat soubor java.security .

Postup

1. Do konfiguračního souboru přidejte následující volby:

Header	Popis
`crl.ldap.host=`*host_name*	Název hostitele LDAP.

Header	Popis
`crl.ldap.port=`*`port_number`*	Číslo portu serveru LDAP. Můžete uvést až 11 serverů. K zajištění transparentního překonání selhání v případě selhání připojení LDAP se používá více hostitelů LDAP. Očekává se, že všechny servery LDAP jsou repliky a obsahují stejná data. Když se zachytávač AMS Java úspěšně připojí k serveru LDAP, nepokusí se stáhnout seznamy CRL ze zbývajících poskytnutých serverů. Produkt Java nepoužívá hodnoty `crl.ldap.user` a crl.ldaworldp.pass . Při připojování k serveru LDAP nepoužívá uživatele a heslo. V důsledku toho musí být atributy CRL v LDAP čitelné pro všechny.
`crl.cdp=on/off`	Pomocí této volby můžete v certifikátech zaškrtnout nebo použít rozšíření CRLDistributionPoints .

2. Upravte soubor `JRE/lib/security/java.security` pomocí následujících vlastností:

Název vlastnosti	Popis
`com.ibm.security.enableCRLDP`	Tato vlastnost má následující hodnoty: `true`, `false`. Je-li nastavena na hodnotu `true`, při provádění kontroly odvolání certifikátu jsou seznamy CRL vyhledány pomocí URL z rozšíření distribučních míst seznamu CRL certifikátu. Je-li nastavena na hodnotu `false` nebo není-li nastavena, je kontrola seznamu CRL pomocí rozšíření distribučních bodů seznamu CRL zakázána.
`ibm.security.certpath.ldap.cache.lifetime`	Tuto vlastnost lze použít k nastavení životnosti položek v mezipaměti LDAP CertStore na hodnotu v sekundách. Hodnota 0 zakáže mezipaměť; hodnota -1 znamená neomezenou dobu životnosti. Není-li nastaveno, výchozí doba trvání je 30 sekund.

Název vlastnosti	Popis
`com.ibm.security.enableAIAEXT`	Tato vlastnost má následující hodnoty: `true`, `false`. Je-li nastavena na hodnotu `true`, všechna rozšíření přístupu k informacím o oprávnění, která se nacházejí v certifikátech cesty k certifikátu, která se sestavují, se prozkoumají, aby se zjistilo, zda obsahují identifikátory URI LDAP. Pro každý nalezený identifikátor URI LDAP se vytvoří objekt LDAPCertStore a přidá se do kolekce CertStores , která se používá k vyhledání dalších certifikátů, které jsou nezbytné pro sestavení cesty k certifikátu. Pokud je nastavena na hodnotu `false` nebo není nastavena, další objekty LDAPCertStore se nevytvoří.

z/OS *Povolení seznamů odvolaných certifikátů (CRL) v systému z/OS*

Produkt Advanced Message Security podporuje kontrolu seznamu odvolaných certifikátů (CRL) digitálních certifikátů používaných k ochraně datových zpráv

Informace o této úloze

Je-li tato volba povolena, produkt Advanced Message Security ověří certifikáty příjemce při vložení zpráv do fronty chráněné ochranou soukromí a certifikáty odesilatele při načtení zpráv z chráněné fronty (integrita nebo soukromí). Validace v tomto případě zahrnuje ověření, že příslušná osvědčení nejsou registrována v příslušné referenční laboratoři Společenství.

Produkt Advanced Message Security používá služby zabezpečení SSL systému IBM k ověřování certifikátů odesilatele a příjemce. Podrobnou dokumentaci týkající se ověření certifikátu SSL systému naleznete v příručce z/OS Cryptographic Services System Secure Sockets Layer Programming .

Chcete-li povolit kontrolu CRL, určete umístění konfiguračního souboru CRL prostřednictvím CRLFILE DD v JCL spuštěné úlohy pro adresní prostor AMS. Ukázkový konfigurační soubor CRL, který lze upravit, je uveden v souboru *thlqual*.SCSQPROC (CSQ40CRL). V tomto souboru jsou povolena následující nastavení:

Tabulka 106. Advanced Message Security proměnné konfigurace CRL

Proměnná	Platné hodnoty	Popis
crl.ldap.host[.n]	*hostname -or-hostname: port*	Adresa IP/název hostitele serveru LDAP, který je hostitelem seznamů CRL certifikátů vydavatele. Pokud neuvedete číslo portu pro server LDAP, použije se číslo portu uvedené v souboru crl.ldap.port .
crl.ldap.port	*port*	Číslo portu TCP/IP vašeho serveru LDAP.
crl.ldap.user	*ldap_user*	Jméno uživatele LDAP, které se má použít při připojování k serveru LDAP.
crl.ldap.pass	*ldap_password*	Heslo LDAP přidružené k souboru crl.ldap.user.

Můžete zadat více názvů hostitelů a portů serveru LDAP následujícím způsobem:

```
crl.ldap.host.1 = hostname -or hostname:port
crl.ldap.host.2 = hostname -or hostname:port
crl.ldap.host.3 = hostname -or hostname:port
```

Můžete uvést až 10 názvů hostitelů. Pokud neuvedete číslo portu pro vaše servery LDAP, použije se číslo portu uvedené v souboru crl.ldap.port . Každý server LDAP musí pro přístup používat stejnou kombinaci crl.ldap.user/password .

Je-li určena definice dat CRLFILE, je konfigurace načtena během inicializace adresního prostoru Advanced Message Security a kontrola CRL je povolena. Není-li určena definice dat CRLFILE, nebo není-li konfigurační soubor CRL k dispozici, nebo je neplatný, je kontrola CRL zakázána.

Produkt AMS provádí kontrolu CRL pomocí služeb ověření certifikátu SSL systému IBM následujícím způsobem:

Tabulka 107. Advanced Message Security kontroly CRL

Operace	**Kvalita ochrany**	**Certifikát (y) zkontrolován (y)**
PUT	Ochrana soukromí	Příjemci
GET	Integrita/Ochrana osobních údajů	Odesílatel

Pokud operace se zprávou selže, kontrola CRL Advanced Message Security provede následující akce:

Tabulka 108. Advanced Message Security Chování při selhání kontroly CRL

Operace	**Selhání kontroly CRL**
PUT	Zpráva není vložena do cílové fronty. Aplikaci byl vrácen kód dokončení MQCC_FAILED a kód příčiny MQRC_SECURITY_ERROR.
GET	Zpráva je odebrána z cílové fronty a přesunuta do fronty chyb ochrany systému. Aplikaci byl vrácen kód dokončení MQCC_FAILED a kód příčiny MQRC_SECURITY_ERROR.

AMS pro z/OS používá IBM systémové služby SSL k ověření certifikátů, což zahrnuje kontrolu CRL a důvěryhodnosti.

Produkt IBM MQ používá nastavení zabezpečení, kde ověření platnosti certifikátu vyžaduje, aby byl server LDAP kontaktovatelný, ale nevyžaduje definování seznamu CRL.

Poznámka: Správci jsou povinni zajistit dostupnost příslušných služeb LDAP a udržovat záznamy CRL pro příslušné certifikační autority.

Nastavení AMS ochrany heslem pro konfigurační soubory

Ukládání hesel úložiště klíčů a soukromých klíčů jako prostého textu představuje bezpečnostní riziko, takže produkt Advanced Message Security poskytuje nástroj, který může tato hesla použít pomocí klíče uživatele.

Než začnete

Vlastník souboru `keystore.conf` se musí ujistit, že pouze vlastník souboru má oprávnění ke čtení a zápisu do souboru. Ochrana hesel popsaná v tomto tématu je pouze dalším měřítkem ochrany. Dále byste měli provést tento postup na zabezpečeném systému.

V 9.3.0 Ujistěte se, že používáte správnou variantu **runamscred** pro typ klienta AMS , který bude číst konfigurační soubor. Pokud je klient AMS :

- Klient Java by měl použít příkaz Java **runamscred** , který je umístěn v adresáři <IBM MQ installation root>/java/bin .
- Klient MQI by měl používat příkaz MQI **runmqascred** umístěný v adresáři <IBM MQ installation root>/bin .

Postup

1. Upravte soubory keystore.conf tak, aby zahrnovaly všechny požadované informace, včetně hesel, která vyžadují ochranu.

```
jceks.keystore = c:/Documents and Settings/Alice/AliceKeystore
jceks.certificate = AliceCert
jceks.encrypted = no
jceks.keystore_pass = passw0rd
jceks.key_pass = passw0rd
jceks.provider = IBMJCE
```

2. Umístěte šifrovací klíč, abyste zašifrovali hesla uvnitř souboru, který je přístupný pro uživatele chránící soubor keystore.conf .

   V 9.3.0 Tento klíč musí být stejný klíč, který bude později použit klientem AMS :

```
ThisIsAnExampleEncryptionKey
```

3. Spusťte příkaz **runamscred** , chcete-li chránit soubor keystore.conf poskytující soubor šifrovacího klíče.

```
runamscred -f <location of keystore.conf> -sf <location of encryption keyfile>
```

4. Ověřte, že byl soubor keystore.conf chráněn a obsahuje šifrovaná hesla.

Příklad

Následující příklad ukazuje, jak chráněný soubor keystore.conf vypadá:

```
jceks.keystore = c:/Documents and Settings/Alice/AliceKeystore
jceks.certificate = AliceCert
jceks.encrypted = yes
jceks.keystore_pass =
<AMS>1!62K/a4RinT+bks4RjFWx4A==!Vhi/RjIN2FH5qStUJ/0hsgKyn2IdMuhanemRRDrJq
HM=
jceks.key_pass =
<AMS>1!qmnxY++rsOUtZfDSgwcR1g==!VmWVREdVkNp1xYJstvuW64ph5vxxf7SPoqtsXxYh2
Tk=
jceks.provider = IBMJCE
```

Související informace

runamscred: chránit AMS klíčová slova

z/OS Použití certifikátů s AMS on z/OS

Informace o této úloze

Advanced Message Security implementuje tři úrovně ochrany: integritu, důvěrnost a soukromí.

Se zásadou integrity jsou zprávy podepsány pomocí soukromého klíče původce (aplikace provádějící příkaz MQPUT). Integrita poskytuje detekci modifikace zprávy, ale samotný text zprávy není šifrován.

Při použití zásady důvěrnosti je zpráva při vložení do fronty zašifrována. Zpráva je šifrována pomocí symetrického klíče a algoritmu uvedeného v příslušné zásadě Advanced Message Security . Samotný symetrický klíč je šifrován pomocí veřejného klíče každého příjemce (aplikace provádějící příkaz MQGET). Veřejné klíče jsou přidruženy k certifikátům uloženým ve sdruženích klíčů.

Se zásadami ochrany osobních údajů jsou zprávy podepsané i šifrované.

Je-li zpráva, která je chráněna s ochranou soukromí, vyřazena z fronty přijímající aplikací, která provádí příkaz MQGET, musí být tato zpráva dešifrována. Protože byl zašifrován pomocí veřejného klíče příjemce, musí být dešifrován pomocí soukromého klíče příjemce nalezeného v svazku klíčů.

z/OS *Použití svazku klíčů SAF s volbou AMS on z/OS*

Advanced Message Security (AMS) používá služby svazku klíčů SAF z/OS k definování a správě certifikátů potřebných pro podepisování a šifrování. Produkty zabezpečení, které jsou funkčně ekvivalentní produktu RACF , mohou být použity místo produktu RACF , pokud poskytují stejnou úroveň podpory.

Efektivní využití klíčových kroužků může snížit potřebu administrace pro správu certifikátů.

Po vygenerování (nebo importu) certifikátu musí být připojen ke svazku klíčů, aby byl přístupný. Stejný certifikát lze připojit k více než jednomu svazku klíčů.

Produkt Advanced Message Security používá dvě sady kroužků klíčů. Jedna sada se skládá ze skupin klíčů vlastněných jednotlivými ID uživatelů, které odesílají nebo přijímají zprávy. Každý svazek klíčů obsahuje soukromý klíč přidružený k certifikátu vlastnícího ID uživatele. Soukromý klíč každého certifikátu se používá k podepisování zpráv pro fronty chráněné ochranou integrity nebo ochranou soukromí. Používá se také k dešifrování zpráv z front chráněných ochranou soukromí nebo ochranou důvěrnosti při přijímání zpráv.

Druhou sadou je jeden svazek klíčů vlastněný uživatelem adresního prostoru AMS . Obsahuje řetězec podpisových certifikátů CA nezbytných pro ověření certifikátů původce zprávy a příjemců.

Při použití ochrany soukromí nebo důvěrnosti obsahuje svazek klíčů vlastněný uživatelem adresního prostoru AMS také certifikáty příjemců zpráv. Veřejné klíče v těchto certifikátech se používají k zašifrování symetrického klíče, který byl použit k zašifrování dat zprávy, když byla zpráva vložena do chráněné fronty. Když jsou tyto zprávy načteny, soukromý klíč příslušných příjemců se použije k dešifrování symetrického klíče, který se pak použije k dešifrování dat zprávy.

Produkt Advanced Message Security používá při hledání certifikátů a soukromých klíčů název svazku klíčů **drq.ams.keyring** . Toto je případ jak pro uživatele, tak pro svazky klíčů adresního prostoru AMS .

Ilustrace a další vysvětlení certifikátů a svazku klíčů a jejich role v ochraně dat viz Souhrn operací souvisejících s certifikáty.

Soukromý klíč použitý pro podepisování může mít libovolný popisek, ale musí být připojen jako výchozí certifikát. Před opravou APAR PH44820může mít soukromý klíč použitý pro dešifrování libovolný popisek, ale musí být připojen jako výchozí certifikát. Je-li použita oprava APAR PH44820 , soukromý klíč nebo klíče použité pro dešifrování mohou mít libovolný popisek a musí být připojeny ke svazku klíčů, ale již nemusí být připojeny jako výchozí certifikát.

Digitální certifikáty a svazky klíčů jsou spravovány v produktu RACF primárně pomocí příkazu RACDCERT.

Další informace o certifikátech, jmenovkách a příkazu RACDCERT naleznete v příručce *z/OS: Security Server RACF Command Language Reference* a *z/OS: Security Server RACF Security Administrator's Guide*.

z/OS *Nahrazení certifikátů*

Když je certifikát obnoven nebo nahrazen (například když se stávající certifikát blíží datu vypršení platnosti), není vždy možné odebrat ochranu z existujících zpráv, které jsou již ve frontách chráněných zásadami důvěrnosti nebo ochrany osobních údajů.

K tomu může dojít, když byl certifikát:

- Obnoveno se stejným soukromým klíčem a znovu vydaný certifikát nahradil původní certifikát
- Překlíčovaný s novým soukromým klíčem a příkaz RACDCERT ROLLOVER odstranil původní soukromý klíč

Před opravou APAR PH44820, když je nový certifikát připojen ke svazku klíčů uživatele jako výchozí certifikát, již není možné dešifrovat zprávy zašifrované pomocí starého certifikátu. Je-li použita oprava APAR PH44820 , budou zprávy dešifrovány za předpokladu, že je nezbytný certifikát připojen ke svazku klíčů uživatele; již není vyžadováno, aby byl připojen jako výchozí. To umožňuje, aby zprávy, které jsou již ve frontě, když je nový certifikát připojen, byly úspěšně dešifrovány.

Následující příklad ukazuje, jak lze vygenerovat nový certifikát na základě existujícího certifikátu při použití opravy APAR PH44820 :

- Vytvoří se nový certifikát na základě existujícího certifikátu s novou dvojicí veřejného/soukromého klíče.
- Nový certifikát je podepsán vydávající autoritou.
- Veřejný klíč starého certifikátu je odebrán ze svazku klíčů adresního prostoru AMS a je přidán veřejný klíč nového certifikátu.
- Kromě starého certifikátu se do svazku klíčů uživatele přidá nový certifikát a soukromý klíč.

```
RACDCERT ID(user1) REKEY(LABEL('user1'))          -
         WITHLABEL('user1new')

RACDCERT GENREQ(LABEL('user1new')) ID(user1)      -
         DSN(output_data_set_name)

RACDCERT GENCERT(output_data_set_name) ID(user1)  -
         SIGNWITH(CERTAUTH LABEL('AMSCA'))

RACDCERT ID(user1) ALTER (LABEL('user1new'))      -
         TRUST

RACDCERT ID(WMQAMSD) REMOVE(ID(user1)             -
         LABEL('user1')                           -
         RING(drq.ams.keyring)  )

RACDCERT ID(WMQAMSD) CONNECT(ID(user1)            -
         LABEL('user1new') USAGE(SITE)            -
         RING(drq.ams.keyring)  )

RACDCERT ID(user1) CONNECT(ID(user1)              -
         LABEL('user1new') USAGE(PERSONAL)        -
         RING(drq.ams.keyring) DEFAULT )
```

Další informace o certifikátech, jmenovkách a příkazu RACDCERT naleznete v příručce *z/OS: Security Server RACF Command Language Reference* a *z/OS: Security Server RACF Security Administrator's Guide*.

z/OS *Autorizace přístupu k příkazu RACDCERT pro AMS on z/OS*

Autorizace k použití příkazu RACDCERT je úloha po instalaci, kterou měl provést systémový programátor z/OS . Tato úloha zahrnuje udělení příslušných oprávnění administrátorovi zabezpečení Advanced Message Security .

Jako souhrn jsou zapotřebí tyto příkazy pro povolení přístupu k příkazu RACF RACDCERT:

```
RDEFINE FACILITY IRR.DIGTCERT.* UACC(NONE)
PERMIT IRR.DIGTCERT.* CLASS(FACILITY) ID( admin ) ACCESS(CONTROL)
SETROPTS RACLIST(FACILITY) REFRESH
```

V tomto příkladu *admin* určuje ID uživatele vašeho administrátora zabezpečení nebo libovolného uživatele, kterého chcete použít s příkazem RACDCERT.

z/OS *Vytvoření certifikátů a kroužků klíčů pro uživatele AMS na systému z/OS*

Tento oddíl dokumentuje kroky nezbytné pro vytvoření certifikátů a klíčových kroužků, které jsou nezbytné pro z/OS uživatele produktu Advanced Message Security (AMS), pomocí certifikační autority (CA) RACF .

Řešení problémů s certifikáty při použití Advanced Message Security na z/OS

Máte-li problémy s certifikáty a chybějícími položkami v úložištích klíčů, můžete povolit trasování GSKIT.

V souboru, na který odkazuje ENVARS DD v proceduře spuštěné úlohy AMS , přidejte:

```
GSK_TRACE_FILE=/u/... /gsktrace
GSK_TRACE=0xff
```

Další informace viz Proměnné prostředí .

Pro každý přístup k úložišti klíčů se data zapisují do trasovacího souboru uvedeného v souboru GSK_TRACE_FILE.

Chcete-li formátovat trasovací soubor, použijte příkaz:

```
gsktrace inputtrace file > output_file
```

Scénář

Scénář odesílající a přijímající aplikace se používá k vysvětlení požadovaných kroků.

V následujících příkladech je user1 původcem zprávy a user2 je příjemcem. ID uživatele Advanced Message Security adresního prostoru je WMQAMSD.

Všechny příkazy v příkladech, které jsou zde uvedeny, jsou vydány z ISPF volba 6 ID administrativního uživatele admin.

z/OS *Definování lokálního certifikátu certifikační autority pro AMS na z/OS*

Používáte-li produkt RACF jako svého CA, musíte vytvořit certifikát certifikační autority, pokud jste tak dosud neučinili. Zde zobrazený příkaz vytvoří certifikát certifikační autority (nebo podepisujícího subjektu). Tento příklad vytvoří certifikát s názvem AMSCA, který se použije při vytváření následných certifikátů, které odrážejí identitu uživatelů a aplikací Advanced Message Security .

Tento příkaz lze upravit, konkrétně SUBJECTSDN, tak, aby odrážel strukturu pojmenování a konvence použité ve vaší instalaci:

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('AMSCA') O('ibm') C('us'))
KEYUSAGE(CERTSIGN) WITHLABEL('AMSCA')
```

Poznámka: Certifikáty podepsané tímto certifikátem lokální certifikační autority zobrazují vydavatele CN=AMSCA, O=ibm, C=us, když jsou uvedeny s příkazem RACDCERT LIST.

z/OS *Vytvoření digitálního certifikátu se soukromým klíčem pro AMS na z/OS*

Digitální certifikát se soukromým klíčem musí být vygenerován pro každého uživatele produktu Advanced Message Security . V níže uvedeném příkladu se příkazy RACDCERT používají ke generování certifikátů pro uživatele user1 a user2, které jsou podepsány certifikátem lokální CA identifikovaným štítkem AMSCA.

```
RACDCERT ID(user1) GENCERT SUBJECTSDN(CN('user1') O('ibm') C('us'))
WITHLABEL('user1') SIGNWITH(CERTAUTH LABEL('AMSCA'))
KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)

RACDCERT ID(user2) GENCERT SUBJECTSDN(CN('user2') O('ibm') C('us'))
WITHLABEL('user2') SIGNWITH(CERTAUTH LABEL('AMSCA'))
KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)

RACDCERT ID(user1) ALTER (LABEL('user1')) TRUST
RACDCERT ID(user2) ALTER (LABEL('user2')) TRUST
```

K přidání atributu TRUST do certifikátu je vyžadován příkaz ALTER RACDCERT. Když je certifikát poprvé vytvořen pomocí tohoto postupu, má jiný platný rozsah dat než podpisový certifikát. V důsledku toho jej RACF označí jako NOTRUST, což znamená, že certifikát se nemá používat. Pomocí příkazu RACDCERT ALTER nastavte atribut TRUST.

Atributy KEYUSAGE HANDSHAKE, DATAENCRYPT a DOCSIGN musí být uvedeny pro certifikáty používané produktem Advanced Message Security.

Tabulka 109. Hodnoty a indikátory RACDCERT KEYUSAGE	
Hodnota KEYUSAGE	**Sada indikátorů**
navázání komunikace	digitalSignature a keyEncipherment
ŠIFROVÁNÍ dat	dataEncipherment
DOCSIGN	nonRepudiation
CERTSIGN	keyCertPodepsat a cRLSign

z/OS *Vytvoření RACF kroužků klíčů pro AMS on z/OS*

Zde zobrazené příkazy vytvoří svazek klíčů pro RACF-defined user IDs user1, user2a uživatele WMQAMSD úlohy adresního prostoru Advanced Message Security . Název svazku klíčů je opraven produktem Advanced Message Security a musí být kódován tak, jak je uvedeno, bez uvozovek. V názvu se rozlišují velká a malá písmena.

```
RACDCERT ID(user1) ADDRING(drq.ams.keyring)
RACDCERT ID(user2) ADDRING(drq.ams.keyring)
RACDCERT ID(WMQAMSD) ADDRING(drq.ams.keyring)
```

z/OS *Připojení certifikátů ke klíčům pro AMS on z/OS*

Připojte certifikáty uživatele a certifikační autority ke klíčovým kroužkům:

```
RACDCERT ID(WMQAMSD) CONNECT(CERTAUTH LABEL('AMSCA')
RING(drq.ams.keyring))
RACDCERT ID(user1) CONNECT(ID(user1) LABEL('user1')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
RACDCERT ID(user2) CONNECT(ID(user2) LABEL('user2')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
RACDCERT ID(WMQAMSD) CONNECT(ID(user2) LABEL('user2')
RING(drq.ams.keyring) USAGE(SITE))
```

Před opravou APAR PH44820musí být certifikát obsahující soukromý klíč použitý pro dešifrování připojen k svazku klíčů uživatele jako výchozí certifikát. Je-li použita oprava APAR PH44820 , všechny certifikáty obsahující soukromý klíč nebo klíče použité pro dešifrování musí být připojeny k svazku klíčů uživatele, avšak již nemusí být připojeny jako výchozí certifikát.

Atribut RACDCERT USAGE (SITE) brání tomu, aby byl soukromý klíč přístupný ve svazku klíčů, zatímco atribut RACDCERT USAGE (PERSONAL) umožňuje použití soukromého klíče, pokud existuje. Certifikát uživatele User2musí být připojen ke svazku klíčů adresního prostoru Advanced Message Security , protože jeho veřejný klíč je potřebný k šifrování zpráv při jejich vložení do fronty. USAGE (SITE) omezuje vystavení soukromého klíče uživatele user2.

Certifikát CERTAUTH s popiskem AMSCA musí být připojen ke svazku klíčů adresního prostoru Advanced Message Security , protože byl použit k podepsání certifikátu user1, který je původcem zprávy. Používá se k ověření podpisového certifikátu uživatele user1.

z/OS *Ověření svazku klíčů pro AMS on z/OS*

Svazek klíčů by se měl objevit tak, jak je zobrazeno zde, po zadání všech příkazů:

```
RACDCERT ID(user1) LISTRING(drq.ams.keyring)
Digital ring information for user USER1:
Ring:>drq.ams.keyring<:

Certificate Label Name           Cert Owner   USAGE    DEFAULT
------------------------------ ------------ -------- -------
user1                            ID(USER1)    PERSONAL YES

RACDCERT ID(user2) LISTRING(drq.ams.keyring)
```

```
Digital ring information for user USER2:
Ring:>drq.ams.keyring<:

Certificate Label Name           Cert Owner   USAGE    DEFAULT
------------------------------ ------------ -------- -------
user2                          ID(USER2)    PERSONAL YES

RACDCERT ID(WMQAMSD) LISTRING(drq.ams.keyring)
Digital ring information for user WMQAMSD:
Ring:>drq.ams.keyring<:

Certificate Label Name           Cert Owner   USAGE    DEFAULT
------------------------------ ------------ -------- -------
AMSCA                          CERTAUTH     CERTAUTH NO
user2                          ID(USER2)    SITE     NO
```

Výpis jednotlivých certifikátů také zobrazuje přidružení kruhu.

```
RACDCERT ID(user2) LIST(label('user2'))
Digital certificate information for user USER2:

***
Label: user2
Certificate ID: 2QfH8Pny9/LzpKKFmfFA
Status: TRUST
Start Date: 2010/05/03 22:59:53
End Date:  2011/05/04 22:59:52
Serial Number:>15<:
Issuer's Name:>OU=AMSCA.O=ibm.C=us<:
Subject's Name:>CN=user2.O=ibm.C=us<:
Key Usage: HANDSHAKE, DATAENCRYPT, DOCSIGN
Private Key Type: Non-ICSF
Private Key Size: 1024
Ring Associations:
Ring Owner: USER2
Ring:>drq.ams.keyring<:
Ring Owner: WMQAMSD
Ring:>drq.ams.keyring<:
```

Pro zlepšení výkonu se obsah souboru drq.ams.keyring přidruženého k adresnímu prostoru AMS ukládá do mezipaměti po dobu životnosti adresního prostoru. Změny v tomto svazku klíčů se neprojeví automaticky. Administrátor může aktualizovat mezipaměť jedním z následujících způsobů:

- Zastavení a restartování správce front.
- Pomocí příkazu z/OS MODIFY:

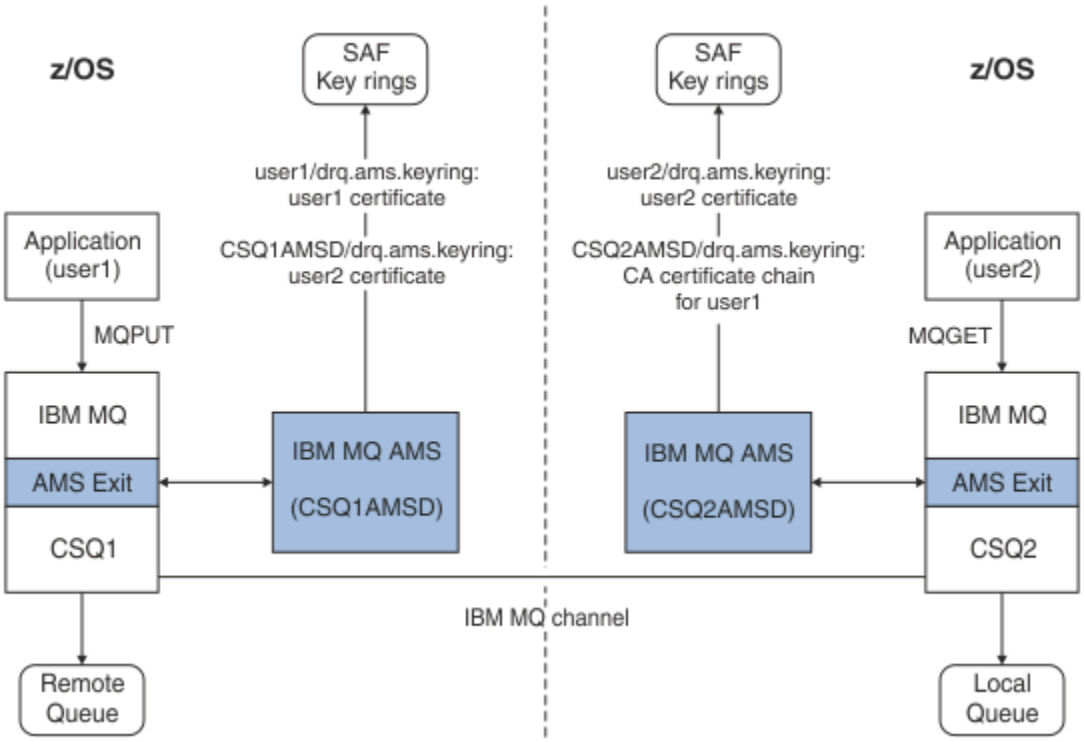
```
F qmgrAMSM,REFRESH KEYRING
```

Související úlohy

Provozní Advanced Message Security

z/OS *Souhrn operací souvisejících s certifikátem pro AMS na z/OS*

Obrázek 35 na stránce 683 ilustruje vztahy mezi odesílajícími a přijímajícími aplikacemi a příslušnými certifikáty. Scénář, který je znázorněn, zahrnuje vzdálené řazení do front mezi dvěma správci front z/OS s použitím zásady ochrany dat. V souboru Obrázek 35 na stránce 683"AMS" označuje " Advanced Message Security".



Obrázek 35. Relace aplikace a certifikátu

V tomto diagramu aplikace spuštěná jako 'user1' vloží zprávu do vzdálené fronty spravované správcem front CSQ1, která má být načtena aplikací spuštěnou jako 'user2' z lokální fronty spravované správcem front CSQ2. Diagram předpokládá zásadu ochrany osobních údajů Advanced Message Security , což znamená, že zpráva je podepsaná i šifrovaná.

Produkt Advanced Message Security zachytí zprávu, když dojde k vložení, a použije certifikát uživatele user2(uložený v svazku klíčů uživatele adresního prostoru AMS) k zašifrování symetrického klíče použitého k zašifrování dat zprávy.

Všimněte si, že certifikát uživatele user2je připojen ke svazku klíčů uživatele adresního prostoru AMS s volbou USAGE (SITE). To znamená, že uživatel adresního prostoru AMS může přistupovat k certifikátu a veřejnému klíči, ale ne k soukromému klíči.

Na přijímacím konci produkt Advanced Message Security zachytí příkaz get vydaný uživatelem user2a použije certifikát uživatele user2k dešifrování symetrického klíče, aby mohl dešifrovat data zprávy. Poté ověří podpis uživatele user1pomocí řetězu certifikátů CA certifikátu user1uloženého v svazku klíčů uživatele adresního prostoru AMS.

Vzhledem k tomuto scénáři, ale se zásadou integrity ochrany dat, nebudou vyžadovány certifikáty pro uživatele user2 .

Chcete-li použít Advanced Message Security k zařazení zpráv do fronty IBM MQ-protected queues, které mají zásadu ochrany zpráv pro ochranu soukromí nebo integrity, Advanced Message Security musí mít přístup k těmto datovým položkám:

- Certifikát X.509 V2 nebo V3 a soukromý klíč pro uživatele, který zprávu zařazuje do fronty.
- Řetěz certifikátů použitých k podepsání digitálních certifikátů všech podepsaných zpráv.
- Pokud je zásada ochrany dat soukromá, certifikát X.509 V2 nebo V3 zamýšlených příjemců. Zamýšlení příjemci jsou uvedeni v zásadě Advanced Message Security přidružené k frontě.

Pro procesy a aplikace, které běží na systému z/OS, musí mít produkt Advanced Message Security certifikáty na dvou místech:

- V svazku klíčů spravovaném zařízením SAF přidruženém k identitě RACF odesílající aplikace (aplikace, která zařadí chráněnou zprávu do fronty) nebo přijímající aplikace (pokud používá soukromí).

  Certifikát, který produkt Advanced Message Security vyhledává, je výchozím certifikátem a musí obsahovat soukromý klíč. Produkt Advanced Message Security předpokládá identitu uživatele z/OS odesílající aplikace. To znamená, že působí jako náhradník, takže má přístup k soukromému klíči uživatele.
- V svazku klíčů spravovaném SAF přidruženém k uživateli adresního prostoru AMS.

  Při odesílání zpráv chráněných ochranou soukromí tento svazek klíčů obsahuje certifikáty veřejných klíčů příjemců zpráv. Při příjmu zpráv obsahuje řetězec certifikátů certifikační autority potřebný k ověření podpisu odesílatele zprávy.

V předchozích příkladech byla jako lokální CA použita položka RACF . Při instalaci však můžete použít jiného poskytovatele PKI (certifikační autoritu). Chcete-li použít jiný produkt PKI, nezapomeňte, že soukromý klíč a certifikát musí být importovány do svazku klíčů přidruženého k ID uživatelů produktu z/OS RACF , která pocházejí ze zpráv IBM MQ chráněných produktem Advanced Message Security.

Můžete použít příkaz RACF RACDCERT jako mechanizmus pro generování žádostí o certifikát, které lze exportovat a odeslat poskytovateli PKI dle vašeho výběru, který má být vydán.

Zde je souhrn kroků souvisejících s certifikátem:

1. Vyžádejte si vytvoření certifikátu CA, ve kterém je RACF lokální CA. Tento krok vynechte, pokud používáte jiného poskytovatele PKI.
2. Vygenerujte uživatelské certifikáty podepsané certifikační autoritou.
3. Vytvořte svazky klíčů pro uživatele a ID adresního prostoru Advanced Message Security AMS.
4. Připojte uživatelský certifikát k svazku klíčů uživatele pomocí výchozího atributu.
5. Připojte certifikáty příjemců k adresnímu svazku adresního prostoru Advanced Message Security AMS pomocí atributu využití (server) (Tento krok je nezbytný pouze pro uživatelské certifikáty, které budou v konečném důsledku příjemci zpráv chráněných ochranou soukromí).
6. Připojte řetězy certifikátů CA pro odesílatele zpráv k svazku klíčů uživatele adresního prostoru Advanced Message Security AMS. (Tento krok je nezbytný pouze pro úlohy AMS, které budou ověřovat podpisy odesílatele.)

z/OS *Konfigurace jiného nežz/OS rezidentního PKI pro AMS*

Advanced Message Security pro systém z/OSpoužívá digitální certifikáty X.509 V3 v ochraně-zpracování zpráv umístěných ve frontách IBM MQ nebo přijatých z front. Produkt Advanced Message Security sám o sobě nevytváří ani nespravuje životní cyklus těchto certifikátů; tuto funkci poskytuje infrastruktura veřejných klíčů (PKI). Příklady v této příručce, které ilustrují použití certifikátů, používají server z/OS Security Server RACF k vyplnění žádostí o certifikáty.

Bez ohledu na to, zda se používá rezidentní PKI z/OS neboz/OS , AMS pro z/OS používá pouze svazky klíčů spravované produktem RACF nebo jeho ekvivalent. Tyto svazky klíčů jsou založeny na prostředku SAF (Security Authorization Facility) a jsou úložištěm, které produkt AMS for z/OS používá k načítání certifikátů pro původce a příjemce zpráv umístěných nebo přijatých z front IBM MQ .

Pro zprávy pocházející z produktu z/OS, které jsou chráněny buď zásadou integrity, nebo zásadou šifrování, musí být certifikát a soukromý klíč původního ID uživatele uloženy v svazku klíčů spravovaném zařízením SAF, který je přidružen k ID uživatele z/OS původce zprávy.

Produkt RACF zahrnuje schopnost importovat certifikáty a soukromé klíče do RACF-spravovaných klíčových kruhů. Podrobnosti a příklady, jak načíst certifikáty do svazky klíčů spravovaných produktem RACF , viz publikace z/OS Security Server RACF .

Pokud vaše instalace používá jeden z podporovaných produktů PKI, podívejte se do příruček, které jsou připojeny k produktu, kde naleznete informace o tom, jak jej implementovat.

Administrace zásad zabezpečení Advanced Message Security

Produkt Advanced Message Security používá zásady zabezpečení k určení šifrovacího šifrování a podpisových algoritmů pro šifrování a ověřování zpráv, které procházejí frontami.

Přehled zásad zabezpečení pro AMS

Zásady zabezpečení produktu Advanced Message Security jsou koncepční objekty, které popisují způsob šifrování a podepisování zprávy.

Podrobnosti o atributech zásad zabezpečení naleznete v následujících dílčích tématech:

Související pojmy

"Kvalita ochrany v AMS" na stránce 689
Zásady ochrany dat Advanced Message Security znamenají kvalitu ochrany (QOP).

"Atributy zásad zabezpečení v adresáři AMS" na stránce 688
Produkt Advanced Message Security můžete použít k výběru konkrétního algoritmu nebo metody pro ochranu dat.

Názvy zásad v souboru AMS

Název zásady je jedinečný název, který identifikuje specifickou zásadu Advanced Message Security a frontu, pro kterou platí.

Název zásady musí být stejný jako název fronty, na kterou se vztahuje. Mezi Advanced Message Security (AMS) existuje mapování jedna ku jedné. zásady a fronty.

Vytvořením zásady se stejným názvem jako fronta aktivujete zásadu pro tuto frontu. Fronty bez odpovídajících názvů zásad nejsou chráněny produktem AMS.

Obor zásady je relevantní pro lokálního správce front a jeho fronty. Vzdálení správci front musí mít vlastní lokálně definované zásady pro fronty, které spravují.

Podpisový algoritmus v AMS

Podpisový algoritmus označuje algoritmus, který by měl být použit při podepisování datových zpráv.

Platné hodnoty:

- MD5
- SHA-1
- SHA-2 Rodina:
  - SHA256
  - SHA384 (minimální přípustná délka klíče-768 bitů)
  - SHA512 (minimální přípustná délka klíče-768 bitů)

Zásada, která neuvádí podpisový algoritmus nebo uvádí algoritmus NONE, znamená, že zprávy umístěné ve frontě přidružené k zásadě nejsou podepsané.

Poznámka: Kvalita ochrany použitá pro funkce vložení a získání zprávy se musí shodovat. Pokud existuje neshoda kvality ochrany mezi frontou a zprávou ve frontě, zpráva nebude přijata a bude odeslána do fronty ošetření chyb. Toto pravidlo platí pro lokální i vzdálené fronty.

Šifrovací algoritmus v souboru AMS

Šifrovací algoritmus označuje algoritmus, který by se měl použít při šifrování datových zpráv umístěných ve frontě přidružené k zásadě.

Platné hodnoty:

- Deprecated RC2
- Deprecated DES

- Deprecated 3DES
- AES128
- AES256

Zásada, která neuvádí šifrovací algoritmus nebo uvádí algoritmus NONE , znamená, že zprávy umístěné ve frontě přidružené k zásadě nejsou šifrovány.

Všimněte si, že zásada, která uvádí jiný šifrovací algoritmus než NONE , musí také uvést alespoň jedno DN příjemce a podpisový algoritmus, protože Advanced Message Security šifrované zprávy jsou také podepsané.

Důležité: Kvalita ochrany použitá pro funkce vložení a získání zprávy se musí shodovat. Pokud existuje neshoda kvality ochrany mezi frontou a zprávou ve frontě, zpráva není přijata a je odeslána do fronty ošetření chyb. Toto pravidlo platí pro lokální i vzdálené fronty.

Tolerance v AMS

Atribut tolerance označuje, zda může produkt Advanced Message Security přijímat zprávy bez zadané zásady zabezpečení.

Při načítání zprávy z fronty se zásadou šifrování zpráv, pokud zpráva není šifrována, je vrácena volající aplikaci. Platné hodnoty:

0
Ne (**výchozí**).

1
Ano.

Zásada, která neurčuje hodnotu tolerance nebo určuje hodnotu 0, znamená, že zprávy umístěné ve frontě přidružené k zásadě musí odpovídat pravidlům zásady.

Tolerance je volitelná a existuje pro usnadnění zavedení konfigurace, kde byly zásady použity na fronty, ale tyto fronty již obsahují zprávy, které nemají uvedenou zásadu zabezpečení.

Rozlišující názvy odesilatelů v souboru AMS

Rozlišující názvy (DN) odesilatele identifikují uživatele, kteří jsou oprávněni umístit zprávy do fronty. Odesílatel používá svůj certifikát k podepsání zprávy před umístěním zprávy do fronty.

Advanced Message Security (AMS) nekontroluje, zda byla zpráva umístěna platným uživatelem do fronty chráněné daty, dokud není zpráva načtena. V tomto okamžiku, pokud zásada určuje jednoho nebo více platných odesilatelů a uživatel, který umístil zprávu do fronty, není v seznamu platných odesilatelů, produkt AMS vrátí chybu přijímající aplikaci a umístí zprávu do fronty chyb AMS.

Pro zásadu může být určeno 0 či více rozlišujících názvů (DN) odesilatelů. Nejsou-li pro zásadu uvedena žádná DN odesilatele, může kterýkoli odesilatel vložit zprávy chráněné daty do fronty za předpokladu, že je certifikát odesilatele důvěryhodný. Certifikát odesílatele je důvěryhodný přidáním veřejného certifikátu do úložiště klíčů, které je k dispozici přijímající aplikaci.

Tvar rozlišujících názvů odesilatelů je následující:

```
CN=Common Name,O=Organization,C=Country
```

Důležité:

- Všechny názvy komponent DN musí být uvedeny velkými písmeny. Všechny identifikátory názvů komponent v DN musí být uvedeny v pořadí uvedeném v následující tabulce:

Název komponenty	Hodnota
CN	Obecný název objektu tohoto DN, například úplný název nebo zamýšlený účel zařízení.

Název komponenty	Hodnota
OU	Jednotka v rámci organizace, ke které je objekt DN přidružen, jako např. divize společnosti nebo název produktu.
O	Organizace, ke které je objekt DN přidružen, například společnost.
L	Lokalita (město nebo obec), kde se nachází objekt DN.
ST	Název státu nebo provincie, kde je umístěn objekt DN.
C	Země, kde je umístěn objekt rozlišujícího názvu (DN).

- Je-li pro zásadu určen jeden či více rozlišujících názvů odesilatelé, mohou do fronty přidružené k příslušné zásadě zařazovat zprávy pouze tito uživatelé.
- Jsou-li určeny rozlišující názvy odesilatelů, musí přesně odpovídat rozlišujícímu názvu uvedenému v digitálním certifikátu přidruženém k uživateli, který zprávu zařadil.
- Produkt AMS podporuje DN s hodnotami pouze ze znakové sady Latin-1 . Chcete-li vytvořit DN se znaky sady, musíte nejprve vytvořit certifikát s DN, který je vytvořen v kódování UTF-8 pomocí AIX and Linux se zapnutým kódováním UTF-8 nebo pomocí grafického rozhraní **strmqikm** . Pak musíte vytvořit zásadu z platformy Linux nebo AIX se zapnutým kódováním UTF-8 nebo použít modul plug-in AMS k IBM MQ.
- Metoda použitá produktem AMSpro převod názvu odesílatele z formátu x.509 na formát DN vždy používá pro hodnotu státu nebo provincie hodnotu ST =.
- Následující speciální znaky vyžadují řídicí znaky:

```
, (comma)
+ (plus)
" (double quote)
\ (backslash)
< (less than)
> (greater than)
; (semicolon)
```

- Pokud rozlišující název obsahuje vložené mezery, měli byste DN uzavřít do dvojitých uvozovek.

Související pojmy

“Rozlišující názvy příjemců v souboru AMS” na stránce 687
Rozlišující názvy (DN) příjemců identifikují uživatele, kteří jsou autorizováni načítat zprávy z fronty.

Rozlišující názvy příjemců v souboru AMS

Rozlišující názvy (DN) příjemců identifikují uživatele, kteří jsou autorizováni načítat zprávy z fronty.

Pro zásadu může být určeno nula či více rozlišujících názvů (DN) příjemců. Rozlišující jména příjemců mají následující tvar:

```
CN=Common Name,O=Organization,C=Country
```

Důležité:

- Všechny názvy komponent DN musí být uvedeny velkými písmeny. Všechny identifikátory názvů komponent v DN musí být uvedeny v pořadí uvedeném v následující tabulce:

Název komponenty	Hodnota
CN	Obecný název objektu tohoto DN, například úplný název nebo zamýšlený účel zařízení.

Název komponenty	Hodnota
OU	Jednotka v rámci organizace, ke které je objekt DN přidružen, jako např. divize společnosti nebo název produktu.
O	Organizace, ke které je objekt DN přidružen, například společnost.
L	Lokalita (město nebo obec), kde se nachází objekt DN.
ST	Název státu nebo provincie, kde je umístěn objekt DN.
C	Země, kde je umístěn objekt rozlišujícího názvu (DN).

- Pokud pro zásadu nejsou určeny žádné rozlišující názvy příjemců, může zprávy z fronty přidružené k příslušné zásadě načítat kterýkoli uživatel.
- Je-li pro zásadu určen jeden či více rozlišujících názvů příjemců, mohou z fronty přidružené k příslušné zásadě načítat zprávy pouze tito uživatelé.
- Jsou-li určeny rozlišující názvy příjemců, musí přesně odpovídat rozlišujícímu názvu uvedenému v digitálním certifikátu přidruženém k uživateli, který zprávu načetl.
- Produkt Advanced Message Security podporuje DN s hodnotami pouze ze znakové sady Latin-1 . Chcete-li vytvořit DN se znaky sady, musíte nejprve vytvořit certifikát s DN, který je vytvořen v kódování UTF-8 pomocí AIX nebo Linux se zapnutým kódováním UTF-8 nebo pomocí grafického rozhraní **strmqikm** . Pak musíte vytvořit zásadu z platformy Linux nebo AIX se zapnutým kódováním UTF-8 nebo použít modul plug-in Advanced Message Security pro IBM MQ.

Související pojmy

“Rozlišující názvy odesilatelů v souboru AMS” na stránce 686

Rozlišující názvy (DN) odesilatele identifikují uživatele, kteří jsou oprávněni umístit zprávy do fronty. Odesílatel používá svůj certifikát k podepsání zprávy před umístěním zprávy do fronty.

Atributy zásad zabezpečení v adresáři AMS

Produkt Advanced Message Security můžete použít k výběru konkrétního algoritmu nebo metody pro ochranu dat.

Zásada zabezpečení je koncepční objekt, který popisuje způsob šifrování a podepisování zprávy.

Tabulka 110. Atributy zásad zabezpečení v adresáři AMS

Atributy	Popis
Název zásady	Jedinečný název zásady pro správce front.
Algoritmus podpisu	Šifrovací algoritmus, který se používá k podepisování zpráv před odesláním.
Šifrovací algoritmus	Šifrovací algoritmus, který se používá k šifrování zpráv před odesláním.
Seznam příjemců	Seznam rozlišujících názvů (DN) certifikátů potenciálních zásobníků zprávy.
Kontrolní seznam rozlišujícího názvu podpisu	Seznam rozlišujících názvů podpisu, které mají být ověřeny během načítání zprávy.

V produktu Advanced Message Securityjsou zprávy šifrovány pomocí symetrického klíče a symetrický klíč je šifrován pomocí veřejných klíčů příjemců. Veřejné klíče jsou šifrovány pomocí algoritmu RSA, s klíči efektivní délky až 2048 bitů. Skutečné asymetrické šifrování klíče závisí na délce klíče certifikátu.

Podporované algoritmy symetrického klíče jsou následující:

- Deprecated RC2
- Deprecated DES
- Deprecated 3DES
- AES128
- AES256

Produkt Advanced Message Security také podporuje následující šifrovací hašovací funkce:

- Deprecated MD5
- Deprecated SHA-1
- SHA-2 Rodina:
  - SHA256
  - SHA384 (minimální přípustná délka klíče-768 bitů)
  - SHA512 (minimální přípustná délka klíče-768 bitů)

Poznámka: Kvalita ochrany použitá pro funkce vložení a získání zprávy se musí shodovat. Pokud existuje neshoda kvality ochrany mezi frontou a zprávou ve frontě, zpráva není přijata a je odeslána do fronty ošetření chyb. Toto pravidlo platí pro lokální i vzdálené fronty.

Kvalita ochrany v AMS

Zásady ochrany dat Advanced Message Security znamenají kvalitu ochrany (QOP).

Tři úrovně kvality ochrany v produktu Advanced Message Security jsou doplněny čtvrtou úrovní v produktu IBM MQ 9.0 a novější a všechny závisí na šifrovacích algoritmech, které se používají k podepsání a šifrování zprávy:

- Soukromí-zprávy umístěné ve frontě musí být podepsány a šifrovány.
- Integrita-zprávy umístěné ve frontě musí být podepsány odesílatelem.
- Důvěrnost-zprávy umístěné ve frontě musí být šifrovány. Další informace naleznete v tématu “Kvalita ochrany k dispozici s AMS” na stránce 614
- Žádná-ochrana dat není použitelná.

Zásada, která určuje, že zprávy musí být podepsány, když jsou umístěny do fronty, má hodnotu QOP INTEGRITY. Hodnota QOP INTEGRITY znamená, že zásada určuje podpisový algoritmus, ale neurčuje šifrovací algoritmus. Na zprávy chráněné integritou se také odkazuje jako na "SIGNED".

Zásada, která určuje, že zprávy musí být podepsány a zašifrovány, když jsou umístěny do fronty, má hodnotu QOP PRIVACY. QOP of PRIVACY znamená, že když zásada stanoví podpisový algoritmus a šifrovací algoritmus. Zprávy chráněné ochranou soukromí jsou také označovány jako "ZAPEČETĚNÉ".

Zásada, která určuje, že zprávy musí být při umístění do fronty šifrovány, má hodnotu QOP DŮVĚRNOST. QOP of DŮVĚRNOST znamená, že zásada určuje šifrovací algoritmus.

Zásada, která neurčuje podpisový algoritmus nebo šifrovací algoritmus, má hodnotu QOP NONE. Produkt Advanced Message Security neposkytuje žádnou ochranu dat pro fronty, které mají zásadu s QOP NONE.

Správa zásad zabezpečení v produktu AMS

Zásada zabezpečení je koncepční objekt, který popisuje způsob šifrování a podepisování zprávy.

Umístění, ze kterého jsou spuštěny všechny administrativní úlohy související se zásadami zabezpečení, závisí na používané platformě.

- ALW V systému AIX, Linux, and Windowsmůžete ke správě zásad zabezpečení použít příkazy DELETE POLICY, DISPLAY POLICYa SET POLICY (nebo ekvivalentní PCF).

  - Linux AIX V systému AIX and Linuxlze administrativní úlohy spouštět z adresáře *MQ_INSTALLATION_PATH*/bin.
  - Windows Na platformách Windows lze administrativní úlohy spouštět z libovolného umístění při aktualizaci proměnné prostředí PATH v instalaci.
- IBM i V systému IBM ijsou příkazy DSPMQMSPL, SETMQMSPLa WRKMQMSPL nainstalovány do knihovny systému QSYS pro primární jazyk systému, když je nainstalován produkt IBM MQ .

  Další národní jazykové verze se instalují do knihoven QSYS29xx podle načtení funkce jazyka. Například počítač s americkou angličtinou jako primárním jazykem a korejštinou jako sekundárním jazykem má příkazy americké angličtiny nainstalované do QSYS a korejské sekundární jazykové zatížení v QSYS2962 jako 2962 je jazykové zatížení pro korejštinu.
- z/OS V systému z/OSjsou administrativní příkazy spouštěny pomocí obslužného programu pro zásady zabezpečení zpráv (CSQ0UTIL). Při vytváření, úpravě nebo odstranění zásad v systému z/OSprodukt Advanced Message Security změny nerozpozná, dokud nebude správce front zastaven a restartován, nebo dokud nebude příkaz z/OS MODIFY použit k aktualizaci konfigurace zásady Advanced Message Security . Příklad:

```
F <qmgr ssid>AMSM,REFRESH POLICY
```

Související úlohy

“Vytvoření zásad zabezpečení v adresáři AMS” na stránce 690
Zásady zabezpečení definují způsob, jakým je zpráva chráněna při vložení zprávy, nebo jak musí být zpráva chráněna při přijetí zprávy.

“Změna zásad zabezpečení v souboru AMS” na stránce 691
Produkt Advanced Message Security můžete použít ke změně podrobností zásad zabezpečení, které jste již definovali.

“Zobrazení a výpis zásad zabezpečení v adresáři AMS” na stránce 692
Pomocí příkazu **dspmqspl** zobrazíte seznam všech zásad zabezpečení nebo podrobnosti o pojmenované zásadě v závislosti na zadaných parametrech příkazového řádku.

“Odebrání zásad zabezpečení v adresáři AMS” na stránce 693
Chcete-li odebrat zásady zabezpečení v produktu Advanced Message Security, musíte použít příkaz `setmqspl` .

Provozní Advanced Message Security

Související odkazy

Obslužný program zásad zabezpečení zpráv (CSQ0UTIL)

Vytvoření zásad zabezpečení v adresáři AMS

Zásady zabezpečení definují způsob, jakým je zpráva chráněna při vložení zprávy, nebo jak musí být zpráva chráněna při přijetí zprávy.

Než začnete

Při vytváření zásad zabezpečení musí být splněny některé vstupní podmínky:

- Správce front musí být spuštěn.
- Název zásady zabezpečení musí splňovat Pravidla pro pojmenování IBM MQ objektů.
- Musíte mít potřebná oprávnění pro připojení ke správci front a vytvořit zásadu zabezpečení:
  - z/OS V systému z/OSudělte oprávnění zdokumentovaná v části Obslužný program zásad zabezpečení zpráv (CSQ0UTIL).
  - Multi Na jiných platformách než z/OSmusíte udělit nezbytná oprávnění + connect, + inq a + chg pomocí příkazu setmqaut .

Další informace o konfiguraci zabezpečení viz “Nastavení zabezpečení” na stránce 131.

- z/OS V systému z/OSse ujistěte, že požadované systémové objekty byly definovány podle definic v CSQ4INSM.

Příklad

Zde je příklad vytvoření zásady ve správci front QMGR. Zásada uvádí, že zprávy budou podepsány pomocí algoritmu SHA256 a zašifrovány pomocí algoritmu AES256 pro certifikáty s DN: CN=joe, O=IBM, C=US a DN: CN=jane, O=IBM, C = US. Tato zásada je připojena k souboru MY.QUEUE:

```
setmqspl -m QMGR -p MY.QUEUE -s SHA256 -e AES256 -r CN=joe,O=IBM,C=US -r CN=jane,O=IBM,C=US
```

Zde je příklad vytvoření zásady ve správci front QMGR. Zásada uvádí, že zprávy jsou šifrovány pomocí algoritmu 3DES pro certifikáty s DN: CN=john, O=IBM, C=US a CN=jeff, O=IBM, C=US a podepsány algoritmem SHA256 pro certifikát s DN: CN=phil, O=IBM, C=US

```
setmqspl -m QMGR -p MY.OTHER.QUEUE -s SHA256 -e 3DES -r CN=john,O=IBM,C=US -r
CN=jeff,O=IBM,C=US -a CN=phil,O=IBM,C=US
```

Poznámka:

- Kvalita ochrany, která se používá pro vložení a získání zprávy, se musí shodovat. Pokud je kvalita ochrany zásady, která je definována pro zprávu, slabší než kvalita definovaná pro frontu, je zpráva odeslána do fronty ošetření chyb. Tato zásada je platná pro lokální i vzdálené fronty.

Související odkazy

Úplný seznam atributů příkazu setmqspl

Změna zásad zabezpečení v souboru AMS

Produkt Advanced Message Security můžete použít ke změně podrobností zásad zabezpečení, které jste již definovali.

Než začnete

- Musí být spuštěn správce front, se kterým chcete pracovat.
- Musíte mít potřebná oprávnění pro připojení ke správci front a vytvoření zásady zabezpečení.
  - z/OS V systému z/OSudělte oprávnění zdokumentovaná v části Obslužný program zásad zabezpečení zpráv (CSQ0UTIL).
  - Multi Na jiných platformách než z/OSmusíte udělit nezbytná oprávnění + connect, + inq a + chg pomocí příkazu setmqaut .

  Další informace o konfiguraci zabezpečení viz “Nastavení zabezpečení” na stránce 131.

Informace o této úloze

Chcete-li změnit zásady zabezpečení, použijte příkaz `setmqspl` na již existující zásadu poskytující nové atributy.

Příklad

Zde je příklad vytvoření zásady s názvem MYQUEUE ve správci front s názvem QMGR, která uvádí, že zprávy mají být šifrovány pomocí algoritmu 3DES pro autory (**-a**), kteří mají certifikáty s rozlišujícím názvem (DN) CN=alice, O=IBM, C=US a podepsány algoritmem SHA256 pro příjemce (**-r**), kteří mají certifikáty s rozlišujícím názvem CN=jeff, O=IBM, C = US.

```
setmqspl -m QMGR -p MYQUEUE -e 3DES -s SHA256 -a CN=jeff,O=IBM,C=US -r CN=alice,O=IBM,C=US
```

Chcete-li změnit tuto zásadu, zadejte příkaz `setmqspl` se všemi atributy z příkladu, který změní pouze hodnoty, které chcete upravit. V tomto příkladu je dříve vytvořená zásada připojena k nové frontě a její šifrovací algoritmus je změněn na AES256:

```
setmqspl -m QMGR -p MYQUEUE -e AES256 -s SHA256 -a CN=jeff,O=IBM,C=US -r CN=alice,O=IBM,C=US
```

Související odkazy

setmqspl (nastavit zásadu zabezpečení)

Zobrazení a výpis zásad zabezpečení v adresáři AMS

Pomocí příkazu **dspmqspl** zobrazíte seznam všech zásad zabezpečení nebo podrobnosti o pojmenované zásadě v závislosti na zadaných parametrech příkazového řádku.

Než začnete

- Chcete-li zobrazit podrobnosti zásad zabezpečení, musí správce front existovat a být spuštěn.
- Musíte mít potřebná oprávnění pro připojení ke správci front a vytvoření zásady zabezpečení.
  - z/OS V systému z/OSudělte oprávnění zdokumentovaná v části Obslužný program zásad zabezpečení zpráv (CSQ0UTIL).
  - Multi Na jiných platformách než z/OSmusíte udělit nezbytná oprávnění + connect, + inq a + chg pomocí příkazu setmqaut .

  Další informace o konfiguraci zabezpečení viz “Nastavení zabezpečení” na stránce 131.

Informace o této úloze

Zde je seznam příznaků příkazu **dspmqspl** :

*Tabulka 111. Příznaky příkazu **dspmqspl** .*

Příznak příkazu	**Vysvětlení**
-m	Název správce front (povinný).
-p	Název zásady.
-export	Přidáním tohoto příznaku se vygeneruje výstup, který lze snadno aplikovat na jiného správce front.

Příklad

Následující příklad uvádí, jak vytvořit dvě zásady zabezpečení pro `venus.queue.manager`:

```
setmqspl -m venus.queue.manager -p AMS_POL_04_ONE -s sha256 -a "CN=signer1,O=IBM,C=US" -e NONE
setmqspl -m venus.queue.manager -p AMS_POL_06_THREE -s sha256 -a "CN=another signer,O=IBM,C=US"
-e NONE
```

Tento příklad zobrazuje příkaz, který zobrazuje podrobnosti o všech zásadách definovaných pro `venus.queue.manager` a výstup, který vytváří:

```
dspmqspl -m venus.queue.manager

Policy Details:
Policy name: AMS_POL_04_ONE
Quality of protection: INTEGRITY
Signature algorithm: SHA256
Encryption algorithm: NONE
Signer DNs:
  CN=signer1,O=IBM,C=US
Recipient DNs: -
Toleration: 0
```

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Policy Details:
Policy name: AMS_POL_06_THREE
Quality of protection: INTEGRITY
Signature algorithm: SHA256
Encryption algorithm: NONE
Signer DNs:
  CN=another signer,O=IBM,C=US
Recipient DNs: -
Toleration: 0
```

Tento příklad zobrazuje příkaz, který zobrazuje podrobnosti o vybrané zásadě zabezpečení definované pro `venus.queue.manager` a výstup, který vytváří:

```
dspmqspl -m venus.queue.manager -p AMS_POL_06_THREE

Policy Details:
Policy name: AMS_POL_06_THREE
Quality of protection: INTEGRITY
Signature algorithm: SHA256
Encryption algorithm: NONE
Signer DNs:
  CN=another signer,O=IBM,C=US
Recipient DNs: -
Toleration: 0
```

V následujícím příkladu nejprve vytvoříme zásadu zabezpečení a pak zásadu exportujete pomocí příznaku **`-export`** :

```
setmqspl -m venus.queue.manager -p AMS_POL_04_ONE -s SHA256 -a "CN=signer1,O=IBM,C=US" -e NONE

dspmqspl -m venus.queue.manager -export
```

z/OS V systému z/OSjsou exportované informace o zásadě zapsány CSQ0UTIL do EXPORT DD.

Multi Na jiných platformách než z/OSpřesměrujte výstup do souboru, například:

```
dspmqspl -m venus.queue.manager -export > policies.[bat|sh]
```

Chcete-li importovat zásadu zabezpečení, postupujte takto:

- Linux AIX V systému AIX and Linux:
  1. Přihlaste se jako uživatel, který patří do skupiny administrace produktu `mqm` IBM MQ .
  2. Vydejte příkaz `. policies.sh`.
- Windows V systému Windowsspusťte příkaz `policies.bat`.
- z/OS V systému z/OS použijte obslužný program CSQ0UTIL a zadejte do SYSIN datovou sadu obsahující exportované informace o zásadě.

Související odkazy

Úplný seznam atributů příkazu dspmqspl

Odebrání zásad zabezpečení v adresáři AMS

Chcete-li odebrat zásady zabezpečení v produktu Advanced Message Security, musíte použít příkaz `setmqspl` .

Než začnete

Při správě zásad zabezpečení musí být splněny některé vstupní podmínky:

- Správce front musí být spuštěn.
- Musíte mít potřebná oprávnění pro připojení ke správci front a vytvoření zásady zabezpečení.

– z/OS V systému z/OSudělte oprávnění zdokumentovaná v části Obslužný program zásad zabezpečení zpráv (CSQ0UTIL).

– Multi Na jiných platformách než z/OSmusíte udělit nezbytná oprávnění + connect, + inq a + chg pomocí příkazu setmqaut .

Další informace o konfiguraci zabezpečení viz “Nastavení zabezpečení” na stránce 131.

Informace o této úloze

Použijte příkaz **setmqspl** s volbou **-remove** .

Příklad

Zde je příklad odebrání zásady:

```
setmqspl -m QMGR -remove -p MY.OTHER.QUEUE
```

Související odkazy

Úplný seznam atributů příkazu setmqspl

Ochrana systémové fronty v produktu AMS

Systémové fronty umožňují komunikaci mezi produktem IBM MQ a jeho pomocnými aplikacemi. Při každém vytvoření správce front je také vytvořena systémová fronta pro ukládání interních zpráv a dat produktu IBM MQ . Systémové fronty můžete chránit pomocí produktu Advanced Message Security , aby k nim mohli přistupovat nebo je dešifrovat pouze autorizovaní uživatelé.

Ochrana systémových front se řídí stejným vzorem jako ochrana běžných front. Viz “Vytvoření zásad zabezpečení v adresáři AMS” na stránce 690.

Windows Chcete-li použít ochranu systémové fronty v systému Windows, zkopírujte soubor `keystore.conf` do následujícího adresáře:

```
c:\Documents and Settings\Default User\.mqs\keystore.conf
```

z/OS Chcete-li v systému z/OSzajistit ochranu pro systém `SYSTEM.ADMIN.COMMAND.QUEUE`, musí mít příkazový server přístup k funkcím `keystore` a `keystore.conf`, které obsahují klíče a konfiguraci, aby mohl příkazový server přistupovat ke klíčům a certifikátům. Všechny změny provedené v zásadách zabezpečení produktu `SYSTEM.ADMIN.COMMAND.QUEUE` vyžadují restart příkazového serveru.

Všechny zprávy, které jsou odesílány a přijímány z fronty příkazů, jsou podepsány nebo podepsány a šifrovány v závislosti na nastavení zásad. Pokud administrátor definuje oprávněné podepisující subjekty, příkazové zprávy, které neprojdou kontrolou rozlišujícího názvu (DN) podepisujícího subjektu, nebudou provedeny příkazovým serverem a nebudou směrovány do fronty ošetření chyb Advanced Message Security . Zprávy odeslané jako odpovědi do dočasných dynamických front produktu IBM MQ Explorer nejsou chráněny produktem AMS.

Zásady zabezpečení nemají vliv na následující fronty SYSTEM:

- SYSTEM.ADMIN.ACCOUNTING.QUEUE
- SYSTEM.ADMIN.ACTIVITY.QUEUE
- SYSTEM.ADMIN.CHANNEL.EVENT
- SYSTEM.ADMIN.COMMAND.EVENT
- z/OS SYSTEM.ADMIN.COMMAND.QUEUE
- SYSTEM.ADMIN.CONFIG.EVENT

- SYSTEM.ADMIN.LOGGER.EVENT
- SYSTEM.ADMIN.PERFM.EVENT
- SYSTEM.ADMIN.PUBSUB.EVENT
- SYSTEM.ADMIN.QMGR.EVENT
- SYSTEM.ADMIN.STATISTICS.QUEUE
- SYSTEM.ADMIN.TRACE.ROUTE.QUEUE
- SYSTEM.AUTH.DATA.QUEUE
- SYSTEM.BROKER.ADMIN.STREAM
- z/OS SYSTEM.BROKER.CLIENTS.DATA
- SYSTEM.BROKER.CONTROL.QUEUE
- SYSTEM.BROKER.DEFAULT.STREAM
- SYSTEM.BROKER.INTER.BROKER.COMMUNICATIONS
- z/OS SYSTEM.BROKER.SUBSCRIPTIONS.DATA
- SYSTEM.CHANNEL.INITQ
- SYSTEM.CHANNEL.SYNCQ
- z/OS SYSTEM.CHLAUTH.DATA.QUEUE
- SYSTEM.CICS.INITIATION.QUEUE
- SYSTEM.CLUSTER.COMMAND.QUEUE
- SYSTEM.CLUSTER.HISTORY.QUEUE
- SYSTEM.CLUSTER.REPOSITORY.QUEUE
- SYSTEM.CLUSTER.TRANSMIT.QUEUE
- z/OS SYSTEM.COMMAND.INPUT
- z/OS SYSTEM.DDELAY.LOCAL.QUEUE
- SYSTEM.DEAD.LETTER.QUEUE
- SYSTEM.DURABLE.SUBSCRIBER.QUEUE
- SYSTEM.HIERARCHY.STATE
- SYSTEM.INTER.QMGR.CONTROL
- SYSTEM.INTER.QMGR.FANREQ
- SYSTEM.INTER.QMGR.PUBS
- SYSTEM.INTERNAL.REPLY.QUEUE
- z/OS SYSTEM.JMS.PS.STATUS.QUEUE
- z/OS SYSTEM.JMS.REPORT.QUEUE
- SYSTEM.PENDING.DATA.QUEUE
- SYSTEM.PROTECTION.ERROR.QUEUE
- SYSTEM.PROTECTION.POLICY.QUEUE
- z/OS SYSTEM.QSG.CHANNEL.SYNCQ
- z/OS SYSTEM.QSG.TRANSMIT.QUEUE
- z/OS SYSTEM.QSG.UR.RESOLUTION.QUEUE
- SYSTEM.RETAINED.PUB.QUEUE
- z/OS SYSTEM.RETAINED.PUB.QUEUE

- SYSTEM.SELECTION.EVALUATION.QUEUE
- SYSTEM.SELECTION.VALIDATION.QUEUE

Multi V 9.3.0 Fronty proudu a AMS

Je možné vysílat duplicitní zprávy chráněné pomocí Advanced Message Security (AMS).

Pokud má fronta definovanou zásadu AMS , která způsobí, že zprávy vkládané do této fronty budou podepsány a/nebo šifrovány, můžete také nakonfigurovat atribut **STREAMQ** fronty tak, aby vložil kopii každé chráněné zprávy do druhé fronty. Duplicitní, kontinuální zpráva je podepsána a/nebo zašifrována pomocí stejné zásady, která byla nakonfigurována pro původní frontu.

V následujícím příkladu konfigurujete dvě fronty, QUEUE1 a QUEUE2. Atribut QUEUE1 má nakonfigurovaný atribut **STREAMQ** pro vložení streamovaných zpráv do QUEUE2:

```
DEFINE QLOCAL(QUEUE2)

DEFINE QLOCAL(QUEUE1) STREAMQ(QUEUE2)
```

AMS chráněné zprávy jsou vkládány do QUEUE1 uživatelem s certifikátem `CN=bob,O=IBM,C=GB`.

Aplikace s certifikátem `CN=alice,O=IBM,C=GB` bude spotřebovávat zprávy z QUEUE1. Samostatná aplikace s certifikátem `CN=fred,O=IBM,C=GB` bude přijímat zprávy z QUEUE2.

QUEUE1 má použité následující AMS zásady ochrany osobních údajů:

```
SET POLICY(QUEUE1) SIGNALG(SHA256) SIGNER('CN=bob,O=IBM,C=GB') ENCALG(AES256)
RECIP('CN=alice,O=IBM,C=GB') RECIP('CN=fred,O=IBM,C=GB') ACTION(ADD)
```

Pokud byl v zásadě nakonfigurován šifrovací algoritmus pro QUEUE1, příjemci uvedení v zásadě musí zahrnovat jak příjemce původních zpráv z QUEUE1, tak i příjemce, kteří budou spotřebovávat duplicitní zprávy z QUEUE2.

Když se aplikace pokusí spotřebovat zprávy z QUEUE2 , provede kontroly integrity a/nebo dešifruje zprávu na základě zásady, která byla nastavena na QUEUE2. Pokud chce aplikace přijímat zprávy s kontinuální relací z QUEUE2, musíte nastavit vhodnou zásadu na QUEUE2 , která umožní, aby byly zprávy kontrolovány na integritu a správně dešifrovány.

Zejména podpisový algoritmus, podepisující subjekt a šifrovací algoritmus musí být stejné jako zásada použitá na QUEUE1. Příjemci zásady pro QUEUE2 musí zahrnovat identitu příjemce, který spotřebovává zprávu z QUEUE2.

Poznámka: Není nutné, aby zásada použitá na QUEUE2 vypsala všechny příjemce uvedené v sadě zásad na QUEUE1.

Například následující zásada může být nastavena na QUEUE2 , aby umožnila aplikaci s rozlišujícím názvem certifikátu `CN=fred,O=IBM,C=GB` číst z ní zprávy chráněné pomocí AMS:

```
SET POLICY(QUEUE2) SIGNALG(SHA256) SIGNER('CN=bob,O=IBM,C=GB') ENCALG(AES256)
RECIP('CN=fred,O=IBM,C=GB') ACTION(ADD)
```

Související pojmy

Fronty proudu

Udělení oprávnění OAM v adresáři AMS

Oprávnění k souborům opravňují všechny uživatele k provádění příkazů `setmqspl` a `dspmqspl` . Produkt Advanced Message Security se však spoléhá na správce OAM (Object Authority Manager) a každý pokus o provedení těchto příkazů uživatelem, který nepatří do skupiny mqm, což je skupina administrace IBM MQ , nebo nemá oprávnění ke čtení nastavení zásad zabezpečení, která jsou udělena, vede k chybě.

Postup

Chcete-li uživateli udělit nezbytná oprávnění, spusťte:

```
setmqaut -m SOME.QUEUE.MANAGER -t qmgr -p SOME.USER +connect +inq
setmqaut -m SOME.QUEUE.MANAGER -t queue -n SYSTEM.PROTECTION.POLICY.QUEUE -p SOME.USER +browse
+put
setmqaut -m SOME.QUEUE.MANAGER -t queue -n SYSTEM.PROTECTION.ERROR.QUEUE -p SOME.USER +put
```

Poznámka: Tato oprávnění OAM je třeba nastavit pouze v případě, že máte v úmyslu připojit klienty ke správci front pomocí produktu Advanced Message Security 7.0.1.

Upozornění: Procházejte oprávnění k systému SYSTEM.PROTECTION.POLICY.QUEUE není povinná ve všech situacích. Produkt IBM MQ optimalizuje výkon ukládáním zásad do mezipaměti, abyste nemuseli procházet záznamy a hledat podrobnosti o zásadách v systému SYSTEM.PROTECTION.POLICY.QUEUE ve všech případech.

Produkt IBM MQ neukládá všechny dostupné zásady do mezipaměti. Pokud existuje vysoký počet zásad, produkt IBM MQ uloží do mezipaměti omezený počet zásad. Pokud má tedy správce front definován nízký počet zásad, není třeba systému SYSTEM.PROTECTION.POLICY.QUEUE.

Měli byste však udělit oprávnění k procházení této fronty v případě, že je definován vysoký počet zásad nebo pokud používáte staré klienty. Systém SYSTEM.PROTECTION.ERROR.QUEUE se používá k vložení chybových zpráv generovaných kódem AMS. Oprávnění vložení pro tuto frontu je kontrolováno pouze při pokusu o vložení chybové zprávy do fronty. Vaše oprávnění pro vložení do fronty není kontrolováno, když se pokusíte vložit nebo získat zprávu z chráněné fronty AMS.

Udělení oprávnění zabezpečení v adresáři AMS

Používáte-li zabezpečení prostředků příkazů, musíte nastavit oprávnění, která umožní funkci produktu Advanced Message Security . Toto téma používá v příkladech příkazy RACF . Pokud váš podnik používá jiného externího správce zabezpečení (ESM), musíte použít ekvivalentní příkazy pro tento ESM.

Udělení oprávnění zabezpečení má tři aspekty:

- “Adresní prostor AMSM” na stránce 697
- “CSQ0UTIL” na stránce 698
- “Použití front, které mají definovanou zásadu Advanced Message Security” na stránce 698

Notes: Ukázkové příkazy používají následující proměnné.

1. *QMgrName* -Název správce front.

   z/OS V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.
2. *username* -Může se jednat o název skupiny.
3. V příkladech je zobrazena třída MQQUEUE. Může to být také MXQUEUE, GMQQUEUE nebo GMXQUEUE. Další informace viz “Profily pro zabezpečení fronty” na stránce 200.

Kromě toho, pokud profil již existuje, nepotřebujete příkaz RDEFINE.

Adresní prostor AMSM

Pro jméno uživatele, pod kterým je spuštěn adresní prostor Advanced Message Security , musíte zadat nějaké zabezpečení IBM MQ .

- Pro dávkové připojení ke správci front zadejte příkaz

```
RDEFINE MQCONN QMgrName.BATCH UACC(NONE)
           PERMIT QMgrName.BATCH CLASS(MQCONN) ID(username) ACCESS(READ)
```

- Pro přístup k systému SYSTEM.PROTECTION.POLICY.QUEUE, vydání:

```
RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE UACC(NONE)
           PERMIT QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(READ)
```

CSQ0UTIL

Obslužný program, který umožňuje uživatelům spouštět příkazy **setmqspl** a **dspmqspl** , vyžaduje následující oprávnění, kde jméno uživatele je ID uživatele úlohy:

- Pro dávkové připojení ke správci front zadejte:

```
  RDEFINE MQCONN QMgrName.BATCH UACC(NONE)
            PERMIT QMgrName.BATCH CLASS(MQCONN) ID(username) ACCESS(READ)
```

- Pro přístup k systému SYSTEM.PROTECTION.POLICY.QUEUE, požadovaná pro příkaz **setmqpol** , zadejte:

```
  RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE UACC(NONE)
              PERMIT QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(ALTER)
```

- Pro přístup k systému SYSTEM.PROTECTION.POLICY.QUEUE, požadovaná pro příkaz **dspmqpol** , zadejte:

```
  RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE UACC(NONE)
                PERMIT QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(READ)
```

Použití front, které mají definovanou zásadu Advanced Message Security

Když aplikace provádí jakoukoli práci s frontami, pro které je definována zásada, vyžaduje tato aplikace další oprávnění, aby mohla produkt Advanced Message Security chránit zprávy.

Aplikace vyžaduje:

- Přístup pro čtení v aplikaci SYSTEM.PROTECTION.POLICY.QUEUE. Proveďte to vydáním:

```
RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE UACC(NONE)
          PERMIT QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(READ)
```

- Zadejte přístup k systému SYSTEM.PROTECTION.ERROR.QUEUE. Proveďte to vydáním:

```
RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.ERROR.QUEUE UACC(NONE)
            PERMIT QMgrName.SYSTEM.PROTECTION.ERROR.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(READ)
```

IBM i Nastavení certifikátů a konfiguračního souboru úložiště klíčů pro systém AMS na systému IBM i

První úlohou při nastavování ochrany produktu Advanced Message Security je vytvořit certifikát a přidružit jej k prostředí. Přidružení je konfigurováno prostřednictvím souboru, který je uložen v integrovaném systému souborů (IFS).

Postup

1. Chcete-li vytvořit certifikát podepsaný svým držitelem pomocí nástrojů OpenSSL dodávaných s produktem IBM i, zadejte následující příkaz z prostředí QShell:

   ```
   /QOpenSys/usr/bin/openssl req -x509 -newkey rsa:2048 -keyout
   $HOME/private.pem -out $HOME/mycert.pem -nodes -days 365
   ```

   Příkaz vyzve k zadání různých atributů rozlišujícího názvu pro nový certifikát podepsaný (svým) držitelem, včetně:

   - Obecný název (CN =)
   - Organizace (O =)

- Země (C =)

Tím se vytvoří nešifrovaný soukromý klíč a odpovídající certifikát, a to jak ve formátu PEM (Privacy Enhanced Mail).

Pro jednoduchost stačí zadat hodnoty pro obecný název, organizaci a zemi. Tyto atributy a hodnoty jsou důležité při vytváření zásady.

Další výzvy a atributy lze upravit zadáním vlastního konfiguračního souboru openssl na příkazovém řádku s parametrem **-config** . Další podrobnosti o syntaxi konfiguračního souboru viz dokumentace OpenSSL .

Následující příkaz například přidá další rozšíření certifikátu X.509 v3 :

```
/QOpenSys/usr/bin/openssl req -x509 -newkey rsa:2048
-keyout $HOME/private.pem -out $HOME/mycert.pem -nodes -days 365 -config myconfig.cnf
```

kde myconfig.cnf je proudový soubor ASCII, který obsahuje následující:

```
[req]
distinguished_name = req_distinguished_name
x509_extensions = myextensions

[req_distinguished_name]
countryName = Country Name (2 letter code)
countryName_default = GB
stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = Hants
localityName = Locality Name (eg, city)
localityName_default = Hursley
organizationName = Organization Name (eg, company)
organizationName_default = IBM United Kingdom
organizationalUnitName = Organizational Unit Name (eg, department)
organizationalUnitName_default = IBM MQ Development
commonName = Common Name (eg, Your Name)

[myextensions]
keyUsage = digitalSignature,nonRepudiation,dataEncipherment,keyEncipherment
extendedKeyUsage = emailProtection
```

2. Produkt AMS vyžaduje, aby certifikát i soukromý klíč byly uloženy ve stejném souboru. Chcete-li toho dosáhnout, zadejte následující příkaz:

```
cat $HOME/mycert.pem >> $HOME/private.pem
```

Soubor `private.pem` v adresáři $HOME nyní obsahuje odpovídající soukromý klíč a certifikát, zatímco soubor `mycert.pem` obsahuje všechny veřejné certifikáty, pro které můžete šifrovat zprávy a ověřovat podpisy.

Tyto dva soubory musí být přidruženy k vašemu prostředí vytvořením konfiguračního souboru úložiště klíčů `keystore.conf`ve vašem výchozím umístění.

Standardně produkt AMS vyhledává konfiguraci úložiště klíčů v podadresáři `.mqs` vašeho domovského adresáře.

3. V prostředí QShell vytvořte soubor `keystore.conf` :

```
mkdir -p $HOME/.mqs
echo "pem.private = $HOME/private.pem" > $HOME/.mqs/keystore.conf
echo "pem.public = $HOME/mycert.pem" >> $HOME/.mqs/keystore.conf
echo "pem.password = unused" >> $HOME/.mqs/keystore.conf
```

IBM i *Vytvoření zásady pro AMS na IBM i*

Před vytvořením zásady musíte vytvořit frontu pro uchování chráněných zpráv.

Postup

1. Na příkazovém řádku zadejte příkaz;

   ```
   CRTMQMQ QNAME(PROTECTED) QTYPE(*LCL) MQMNAME (mqmname)
   ```

   kde mqmname je název vašeho správce front.

   Pomocí příkazu DSPMQM zkontrolujte, zda je správce front schopen používat zásady zabezpečení. Ujistěte se, že **Security Policy Capability** zobrazuje **YES*.

   Nejjednodušší zásadou, kterou můžete definovat, je zásada integrity, které je dosaženo vytvořením zásady s algoritmem digitálního podpisu, ale bez šifrovacího algoritmu.

   Zprávy jsou podepsané, ale nejsou šifrované. Mají-li být zprávy šifrovány, musíte zadat šifrovací algoritmus a jednoho nebo více zamýšlených příjemců zprávy.

   Certifikát ve veřejném úložišti klíčů pro zamýšleného příjemce zprávy je identifikován pomocí rozlišujícího názvu.
2. Zobrazte rozlišující názvy certifikátů ve veřejném úložišti klíčů, mycert.pem v $HOME, pomocí následujícího příkazu v prostředí QShell:

   ```
   /QOpenSys/usr/bin/openssl x509 -in $HOME/mycert.pem -noout -subject -nameopt RFC2253
   ```

   Musíte zadat rozlišující název jako zamýšlený příjemce a název zásady se musí shodovat s názvem fronty, která má být chráněna.
3. Na příkazovém řádku CL zadejte například:

   ```
   SETMQMSPL POLICY(PROTECTED) MQMNAME (mqmname)SIGNALG(*SHA256) ENCALG(*AES256) RECIP('CN=..,
   O=.., C=..')
   ```

   kde mqmname je název vašeho správce front.

   Jakmile je zásada vytvořena, všechny zprávy, které jsou vloženy, procházeny nebo destruktivně odebrány prostřednictvím tohoto názvu fronty, podléhají zásadě AMS .

Související odkazy

Zobrazení správce front zpráv (DSPMQM)

Nastavit zásadu zabezpečení MQM (SETMQMSPL)

IBM i *Testování zásady pro AMS na IBM i*

Pomocí ukázkových aplikací dodávaných s produktem otestujte zásady zabezpečení.

Informace o této úloze

Můžete použít ukázkové aplikace dodávané s produktem IBM MQ , například AMQSPUT4, AMQSGET4, AMQSGBR4a nástroje, jako je WRKMQMMSG, pro vložení, procházení a získání zpráv pomocí názvu fronty PROTECTED.

Za předpokladu, že vše bylo správně nakonfigurováno, neměl by být žádný rozdíl v chování aplikace vůči nechráněné frontě pro tohoto uživatele.

Uživatel, který není nastaven pro produkt Advanced Message Security, nebo uživatel, který nemá požadovaný soukromý klíč pro dešifrování zprávy, však nebude moci zprávu zobrazit. Uživatel obdrží kód dokončení RCFAIL, který je ekvivalentní MQCC_FAILED (2) a kód příčiny RC2063 (MQRC_SECURITY_ERROR).

Chcete-li vidět, že ochrana AMS je v platnosti, vložte některé testovací zprávy do fronty PROTECTED, například pomocí AMQSPUT0. Poté můžete vytvořit alias frontu pro procházení nezpracovaných chráněných dat v klidu.

Postup

Chcete-li uživateli udělit nezbytná oprávnění, spusťte:

```
CRTMQMQ QNAME(ALIAS) QTYPE(*ALS) TGTQNAME(PROTECTED) MQMNAME(yourqm)
```

Procházení pomocí názvu fronty ALIAS, například pomocí AMQSBCG4 nebo WRKMQMMSG, by mělo odhalit větší zprávy `scrambled` , kde procházení fronty PROTECTED zobrazuje zprávy v prostém textu.

Kódované zprávy jsou viditelné, ale původní prostý text není dešifrovatelný pomocí fronty ALIAS, protože neexistuje žádná zásada pro AMS, která by vynucovala shodu s tímto názvem. Proto jsou vrácena nezpracovaná chráněná data.

Související odkazy

Nastavit zásadu zabezpečení MQM (SETMQMSPL)

Práce se zprávami produktu MQ (WRKMQMMSG)

Události příkazu a konfigurace pro AMS

Pomocí produktu Advanced Message Securitymůžete generovat zprávy událostí příkazu a konfigurace, které mohou být protokolovány a sloužit jako záznam změn zásad pro auditování.

Události příkazu a konfigurace generované produktem IBM MQ jsou zprávy ve formátu PCF odeslané do vyhrazených front ve správci front, ve kterém došlo k události.

Zprávy událostí konfigurace se odesílají do SYSTEM.ADMIN.CONFIG.EVENT .

Zprávy událostí příkazu jsou odesílány do SYSTEM.ADMIN.COMMAND.EVENT .

Události jsou generovány bez ohledu na nástroje, které používáte ke správě zásad zabezpečení Advanced Message Security .

V produktu Advanced Message Securityexistují čtyři typy událostí generované různými akcemi v zásadách zabezpečení:

- "Vytvoření zásad zabezpečení v adresáři AMS" na stránce 690, které generují dvě zprávy události IBM MQ :
  - Událost konfigurace
  - Událost příkazu
- "Změna zásad zabezpečení v souboru AMS" na stránce 691, který generuje tři zprávy událostí IBM MQ :
  - Událost konfigurace, která obsahuje staré hodnoty zásad zabezpečení
  - Událost konfigurace, která obsahuje nové hodnoty zásad zabezpečení
  - Událost příkazu
- "Zobrazení a výpis zásad zabezpečení v adresáři AMS" na stránce 692, který generuje jednu zprávu události IBM MQ :
  - Událost příkazu
- "Odebrání zásad zabezpečení v adresáři AMS" na stránce 693, který generuje dvě zprávy události IBM MQ :
  - Událost konfigurace
  - Událost příkazu

Povolení a zakázání protokolování událostí pro AMS

Události příkazů a konfigurace můžete řídit pomocí atributů správce front **CONFIGEV** a **CMDEV**. Chcete-li tyto události povolit, nastavte příslušný atribut správce front na hodnotu POVOLENO. Chcete-li tyto události zakázat, nastavte příslušný atribut správce front na hodnotu DISABLED.

Postup

Události konfigurace

Chcete-li povolit události konfigurace, nastavte parametr **CONFIGEV** na hodnotu ENABLED. Chcete-li zakázat události konfigurace, nastavte parametr **CONFIGEV** na hodnotu DISABLED. Můžete například povolit události konfigurace pomocí následujícího příkazu MQSC:

```
ALTER QMGR CONFIGEV (ENABLED)
```

Události příkazů

Chcete-li povolit události příkazu, nastavte parametr **CMDEV** na hodnotu ENABLED. Chcete-li povolit události příkazů pro příkazy kromě příkazů **DISPLAY MQSC** a příkazů Inquire PCF, nastavte parametr **CMDEV** na hodnotu NODISPLAY. Chcete-li zakázat události příkazu, nastavte parametr **CMDEV** na hodnotu DISABLED. Můžete například povolit události příkazů pomocí následujícího příkazu MQSC:

```
ALTER QMGR CMDEV (ENABLED)
```

Související úlohy

Řízení událostí konfigurace, příkazu a modulu protokolování v produktu IBM MQ

Formát zprávy události příkazu pro AMS

Zpráva události příkazu se skládá ze struktury MQCFH a parametrů PCF, které následují.

Zde jsou vybrané hodnoty MQCFH:

```
Type = MQCFT_EVENT;
Command = MQCMD_COMMAND_EVENT;
MsgSeqNumber = 1;
Control = MQCFC_LAST;
ParameterCount = 2;
CompCode = MQCC_WARNING;
Reason = MQRC_COMMAND_PCF;
```

Poznámka: Hodnota ParameterCount je dvě, protože vždy existují dva parametry typu MQCFGR (skupina). Každá skupina se skládá z příslušných parametrů. Data události se skládají ze dvou skupin, CommandContext a CommandData.

CommandContext obsahuje:

EventUserId

Popis:	ID uživatele, pod kterým byl spuštěn příkaz nebo volání, které událost vygenerovalo. (Jedná se o stejné ID uživatele, které se používá ke kontrole oprávnění k vydání příkazu nebo volání; pro příkazy přijaté z fronty se jedná také o identifikátor uživatele (UserIdentifier) z MD zprávy příkazu).
Identifikátor:	MQCACF_EVENT_USER_ID.
Datový typ:	MQCFST.
Maximální délka:	MQ_USER_ID_LENGTH.
Vráceno:	Vždy.

EventOrigin

Popis:	Původ akce způsobující událost.
Identifikátor:	MQIACF_EVENT_ORIGIN.
Datový typ:	MQCFIN.

Hodnoty:

MQEVO_CONSOLE
Příkazový řádek konzoly.

MQEVO_MSG
Zpráva příkazu z modulu plug-in IBM MQ Explorer .

Vráceno: Vždy.

EventQMgr

Popis: Správce front, kde byl zadán příkaz nebo volání. (Správce front, kde je příkaz proveden a který generuje událost, je v MD zprávy události).

Identifikátor: MQCACF_EVENT_Q_MGR.

Datový typ: MQCFST.

Maximální délka: MQ_Q_MGR_NAME_LENGTH.

Vráceno: Vždy.

EventAccountingToken

Popis: Pro příkazy přijaté jako zpráva (MQEVO_MSG), token evidence (AccountingToken) z MD zprávy příkazu.

Identifikátor: MQBACF_EVENT_ACCOUNTING_TOKEN.

Datový typ: MQCFBS.

Maximální délka: MQ_ACCOUNTING_TOKEN_LENGTH.

Vráceno: Pouze v případě, že EventOrigin je MQEVO_MSG.

EventIdentityData

Popis: Pro příkazy přijaté jako zpráva (MQEVO_MSG), data identity aplikace (ApplIdentityData) z MD zprávy příkazu.

Identifikátor: MQCACF_EVENT_APPL_IDENTITY.

Datový typ: MQCFST.

Maximální délka: MQ_APPL_IDENTITY_DATA_LENGTH.

Vráceno: Pouze v případě, že EventOrigin je MQEVO_MSG.

EventApplType

Popis: Pro příkazy přijaté jako zpráva (MQEVO_MSG) se jedná o typ aplikace (PutApplType) z deskriptoru zprávy příkazu.

Identifikátor: MQIACF_EVENT_APPL_TYPE.

Datový typ: MQCFIN.

Vráceno: Pouze v případě, že EventOrigin je MQEVO_MSG.

EventApplName

Popis: Pro příkazy přijaté jako zpráva (MQEVO_MSG) se jedná o název aplikace (PutApplName) z deskriptoru zprávy příkazu.

Identifikátor: MQCACF_EVENT_APPL_NAME.

Datový typ: MQCFST.

Maximální délka: MQ_APPL_NAME_LENGTH.

Vráceno: Pouze v případě, že EventOrigin je MQEVO_MSG.

EventApplOrigin

Popis: Pro příkazy přijaté jako zpráva (MQEVO_MSG) se jedná o data původu aplikace (ApplOriginData) z deskriptoru zprávy příkazu.

Identifikátor: MQCACF_EVENT_APPL_ORIGIN.

Datový typ: MQCFST.

Maximální délka: MQ_APPL_ORIGIN_DATA_LENGTH.

Vráceno: Pouze v případě, že EventOrigin je MQEVO_MSG.

Příkaz

Popis: Kód příkazu.

Identifikátor: MQIACF_COMMAND.

Datový typ: MQCFIN.

Hodnoty: **MQCMD_INQUIRE_PROT_POLICY číselná hodnota 205**
MQCMD_CREATE_PROT_POLICY číselná hodnota 206
MQCMD_DELETE_PROT_POLICY číselná hodnota 207
MQCMD_CHANGE_PROT_POLICY číselná hodnota 208
Ty jsou definovány v IBM MQ 8.0 `cmqcfc.h`

Vráceno: Vždy.

CommandData obsahuje prvky PCF, které tvoří příkaz PCF.

Formát zprávy události konfigurace pro AMS

Události konfigurace jsou zprávy PCF standardního formátu Advanced Message Security .

Možné hodnoty pro deskriptor zprávy MQMD lze nalézt v části Zpráva události MQMD (deskriptor zprávy).

Zde jsou vybrané hodnoty MQMD:

```
Format = MQFMT_EVENT
Peristence = MQPER_PERSISTENCE_AS_Q_DEF
PutApplType = MQAT_QMGR           //for both CLI and command server
```

Vyrovnávací paměť zpráv se skládá ze struktury MQCFH a struktury parametrů, která ji následuje. Možné hodnoty MQCFH naleznete v části Zpráva události MQCFH (záhlaví PCF).

Zde jsou vybrané hodnoty MQCFH:

```
Type = MQCFT_EVENT
Command = MQCMD_CONFIG_EVENT
MsgSeqNumber = 1 or 2          // 2 will be in case of Change Object event
Control = MQCFC_LAST or MQCFC_NOT_LAST     //MQCFC_NOT_LAST will be in case of 1 Change Object
event
ParameterCount = reflects number of PCF parameters following MQCFH
CompCode = MQCC_WARNING
Reason = one of {MQRC_CONFIG_CREATE_OBJECT, MQRC_CONFIG_CHANGE_OBJECT,
MQRC_CONFIG_DELETE_OBJECT}
```

Parametry následující MQCFH jsou:

EventUserID

Popis: ID uživatele, pod kterým byl spuštěn příkaz nebo volání, které událost vygenerovalo. (Jedná se o stejné ID uživatele, které se používá ke kontrole oprávnění k vydání příkazu nebo volání; pro příkazy přijaté z fronty se jedná také o identifikátor uživatele (UserIdentifier) z MD zprávy příkazu).

Identifikátor: **MQCACF_EVENT_USER_ID**

Datový typ: MQCFST.

Maximální délka: MQ_USER_ID_LENGTH.

Vráceno: Vždy.

SecurityId

Popis: Hodnota MQMD.AccountingToken v případě zprávy příkazového serveru nebo Windows SID pro lokální příkaz.

Identifikátor: **MQBACF_EVENT_SECURITY_ID**

Datový typ: MQCBS.

Maximální délka: MQ_SECURITY_ID_LENGTH.

Vráceno: Vždy.

EventOrigin

Popis: Původ akce způsobující událost.

Identifikátor: **MQIACF_EVENT_ORIGIN**

Datový typ: MQCFIN.

Hodnoty:

MQEVO_CONSOLE
Příkazový řádek konzoly.

MQEVO_MSG
Zpráva příkazu z modulu plug-in Průzkumníka IBM MQ .

Vráceno: Vždy.

EventQMgr

Popis: Správce front, kde byl zadán příkaz nebo volání. (Správce front, kde je příkaz proveden a který generuje událost, je v MD zprávy události).

Identifikátor: **MQCACF_EVENT_Q_MGR**

Datový typ: MQCFST

Maximální délka: MQ_Q_NÁZEV_MGR_LENGTH

Vráceno: Vždy.

ObjectType

Popis: Typ objektu.

Identifikátor: **MQIACF_OBJECT_TYPE**

Datový typ: MQCFIN

Hodnota:

MQOT_PROT_POLICY
Advanced Message Security zásady ochrany. **1019** -Číselná hodnota definovaná v produktu IBM MQ 8.0 nebo v souboru `cmqc.h` .

Vráceno: Vždy.

PolicyName

Popis: Název zásady Advanced Message Security .

Identifikátor: **MQCA_POLICY_NAME**.

Datový typ: MQCFST.

Hodnota: **2112** -Číselná hodnota definovaná v produktu IBM MQ 8.0 nebo v souboru `cmqc.h` .

Maximální délka: MQ_OBJECT_NAME_LENGTH.

Vráceno: Vždy.

PolicyVersion

Popis: Verze zásady Advanced Message Security .

Identifikátor: **MQIA_POLICY_VERSION**

Datový typ: MQCFIN

Hodnota **238** -Číselná hodnota definovaná v produktu IBM MQ 8.0 nebo v souboru `cmqc.h` .

Vráceno: Vždy

TolerateFlag

Popis: Příznak tolerance zásady Advanced Message Security .

Identifikátor: **MQIA_TOLERATE_UNPROTECTED**

Datový typ: MQCFIN

Hodnota **235** -Číselná hodnota definovaná v produktu IBM MQ 8.0 nebo v souboru `cmqc.h` .

Vráceno: Vždy.

SignatureAlgorithm

Popis: Podpisový algoritmus zásady Advanced Message Security .

Identifikátor: **Algoritmus MQIA_SIGNATURE_ALGORITHM**

Datový typ: MQCFIN

Hodnota: **236** -Číselná hodnota definovaná v produktu IBM MQ 8.0 nebo v souboru `cmqc.h` .

Vráceno: Kdykoli je v zásadě Advanced Message Security definován podpisový algoritmus

EncryptionAlgorithm

Popis: Šifrovací algoritmus zásady Advanced Message Security .

Identifikátor: **Algoritmus MQIA_ENCRYPTION_ALGORITHM**

Datový typ: MQCFIN

Hodnota: **237** -číselná hodnota definovaná v produktu IBM MQ 8.0 nebo v souboru `cmqc.h` .

Vráceno: Kdykoli je v zásadě IBM MQ definován šifrovací algoritmus.

SignerDNs

Popis:	Předmět DistinguishedName povolených podepisujících subjektů.
Identifikátor:	**MQCA_SIGNER_DN**
Datový typ:	MQCFSL
Hodnota:	**2113** -Číselná hodnota definovaná v produktu IBM MQ 8.0 nebo v souboru `cmqc.h` .
Maximální délka:	Nejdelší rozlišující název podepisujícího subjektu v zásadě, ale již ne MQ_ROZLIŠED_NAME_LENGTH
Vráceno:	Kdykoli je definováno v zásadě IBM MQ .

RecipientDNs

Popis:	Předmět DistinguishedName povolených podepisujících subjektů.
Identifikátor:	**MQCA_RECIPIENT_DN**
Datový typ:	MQCFSL
Hodnota:	**2114** -Číselná hodnota definovaná v produktu IBM MQ 8.0 nebo v souboru `cmqc.h` .
Maximální délka:	Nejdelší rozlišující název příjemce v zásadě, ale již ne MQ_ROZLIŠISHED_NAME_LENGTH.
Vráceno:	Kdykoli je definováno v zásadě IBM MQ .

Poznámky

Tyto informace byly vyvinuty pro produkty a služby poskytované v USA.

Společnost IBM nemusí nabízet produkty, služby nebo funkce uvedené v tomto dokumentu v jiných zemích. Informace o produktech a službách, které jsou ve vaší oblasti aktuálně dostupné, získáte od místního zástupce společnosti IBM. Odkazy na produkty, programy nebo služby společnosti IBM v této publikaci nejsou míněny jako vyjádření nutnosti použití pouze uvedených produktů, programů či služeb společnosti IBM. Místo toho lze použít jakýkoli funkčně ekvivalentní produkt, program nebo službu, které neporušují žádná práva k duševnímu vlastnictví IBM. Ověření funkčnosti produktu, programu nebo služby pocházející od jiného výrobce je však povinností uživatele.

Společnost IBM může vlastnit patenty nebo nevyřízené žádosti o patenty zahrnující předměty popsané v tomto dokumentu. Vlastnictví tohoto dokumentu neposkytuje licenci k těmto patentům. Dotazy týkající se licencí můžete posílat písemně na adresu:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Odpovědi na dotazy týkající se licencí pro dvoubajtové znakové sady (DBCS) získáte od oddělení IBM Intellectual Property Department ve vaší zemi, nebo tyto dotazy můžete zasílat písemně na adresu:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

Následující odstavec se netýká Spojeného království ani jiných zemí, ve kterých je takovéto vyjádření v rozporu s místními zákony: SPOLEČNOST INTERNATIONAL BUSINESS MACHINES CORPORATION TUTO PUBLIKACI POSKYTUJE "TAK, JAK JE" BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH VÝSLOVNĚ NEBO VYPLÝVAJÍCÍCH Z OKOLNOSTÍ, VČETNĚ, A TO ZEJMÉNA, ZÁRUK NEPORUŠENÍ PRÁV TŘETÍCH STRAN, PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL. Některé právní řády u určitých transakcí nepřipouštějí vyloučení záruk výslovně vyjádřených nebo vyplývajících z okolností, a proto se na vás toto omezení nemusí vztahovat.

Uvedené údaje mohou obsahovat technické nepřesnosti nebo typografické chyby. Údaje zde uvedené jsou pravidelně upravovány a tyto změny budou zahrnuty v nových vydáních této publikace. Společnost IBM může kdykoli bez upozornění provádět vylepšení nebo změny v produktech či programech popsaných v této publikaci.

Veškeré uvedené odkazy na webové stránky, které nespravuje společnost IBM, jsou uváděny pouze pro referenci a v žádném případě neslouží jako záruka funkčnosti těchto webů. Materiály uvedené na tomto webu nejsou součástí materiálů pro tento produkt IBM a použití uvedených stránek je pouze na vlastní nebezpečí.

Společnost IBM může použít nebo distribuovat jakékoli informace, které jí sdělíte, libovolným způsobem, který společnost považuje za odpovídající, bez vyžádání vašeho svolení.

Vlastníci licence k tomuto programu, kteří chtějí získat informace o možnostech (i) výměny informací s nezávisle vytvořenými programy a jinými programy (včetně tohoto) a (ii) oboustranného využití vyměňovaných informací, mohou kontaktovat informační středisko na adrese:

IBM Corporation
Koordinátor interoperability softwaru, oddělení 49XA
3605 Dálnice 52 N

Rochester, MN 55901
U.S.A.

Poskytnutí takových informací může být podmíněno dodržením určitých podmínek a požadavků zahrnujících v některých případech uhrazení stanoveného poplatku.

Licencovaný program popsaný v těchto informacích a veškerý licencovaný materiál, který je pro něj k dispozici, jsou poskytovány společností IBM na základě podmínek IBM Smlouvy se zákazníkem, IBM Mezinárodní licenční smlouvy pro programy nebo jiné ekvivalentní smlouvy mezi námi.

Jakékoli údaje o výkonnosti obsažené v této publikaci byly zjištěny v řízeném prostředí. Výsledky získané v jakémkoli jiném operačním prostředí se proto mohou výrazně lišit. Některá měření mohla být prováděna na vývojových verzích systémů a není zaručeno, že tato měření budou stejná i na běžně dostupných systémech. Některá měření mohla být navíc odhadnuta pomocí extrapolace. Skutečné výsledky mohou být jiné. Čtenáři tohoto dokumentu by měli zjistit použitelné údaje pro své specifické prostředí.

Informace týkající se produktů jiných výrobců pocházejí od dodavatelů těchto produktů, z jejich veřejných oznámení nebo z jiných veřejně dostupných zdrojů. Společnost IBM tyto produkty netestovala a nemůže potvrdit správný výkon, kompatibilitu ani žádné jiné výroky týkající se produktů jiných výrobců než IBM. Otázky týkající se kompatibility produktů jiných výrobců by měly být směrovány dodavatelům těchto produktů.

Veškerá tvrzení týkající se budoucího směru vývoje nebo záměrů společnosti IBM se mohou bez upozornění změnit nebo mohou být zrušena a reprezentují pouze cíle a plány společnosti.

Tyto údaje obsahují příklady dat a sestav používaných v běžných obchodních operacích. Aby byla představa úplná, používají se v příkladech jména osob a názvy společností, značek a produktů. Všechna tato jména a názvy jsou fiktivní a jejich podobnost se jmény, názvy a adresami používanými ve skutečnosti je zcela náhodná.

LICENČNÍ INFORMACE:

Tyto informace obsahují ukázkové aplikační programy ve zdrojovém jazyce ilustrující programovací techniky na různých operačních platformách. Tyto ukázkové programy můžete bez závazků vůči společnosti IBM jakýmkoli způsobem kopírovat, měnit a distribuovat za účelem vývoje, používání, odbytu či distribuce aplikačních programů odpovídajících rozhraní API pro operační platformu, pro kterou byly ukázkové programy napsány. Tyto příklady nebyly plně testovány za všech podmínek. Společnost IBM proto nemůže zaručit spolehlivost, upotřebitelnost nebo funkčnost těchto programů.

Při prohlížení těchto dokumentů v elektronické podobě se nemusí zobrazit všechny fotografie a barevné ilustrace.

Informace o programovacím rozhraní

Informace o programovacím rozhraní, jsou-li poskytnuty, jsou určeny k tomu, aby vám pomohly vytvořit aplikační software pro použití s tímto programem.

Tato příručka obsahuje informace o zamýšlených programovacích rozhraních, která zákazníkům umožňují psát programy za účelem získání služeb produktu WebSphere MQ.

Tyto informace však mohou obsahovat i diagnostické údaje a informace o úpravách a ladění. Informace o diagnostice, úpravách a vyladění jsou poskytovány jako podpora ladění softwarových aplikací.

Důležité: Tyto informace o diagnostice, úpravách a ladění nepoužívejte jako programovací rozhraní, protože se mohou měnit.

Ochranné známky

IBM, logo IBM , ibm.com, jsou ochranné známky společnosti IBM Corporation, registrované v mnoha jurisdikcích po celém světě. Aktuální seznam ochranných známek společnosti IBM je k dispozici na webu "Copyright and trademark information"www.ibm.com/legal/copytrade.shtml. Další názvy produktů a služeb mohou být ochrannými známkami společnosti IBM nebo jiných společností.

Microsoft a Windows jsou ochranné známky společnosti Microsoft Corporation ve Spojených státech a případně v dalších jiných zemích.

UNIX je registrovaná ochranná známka skupiny The Open Group ve Spojených státech a případně v dalších jiných zemích.

Linux je registrovaná ochranná známka Linuse Torvaldse ve Spojených státech a případně v dalších jiných zemích.

Tento produkt zahrnuje software vyvinutý projektem Eclipse (https://www.eclipse.org/).

Java a všechny ochranné známky a loga založené na termínu Java jsou ochranné známky nebo registrované ochranné známky společnosti Oracle anebo příbuzných společností.

Číslo položky:

(1P) P/N: