9.2

Zabezpečení produktu IBM MQ

Poznámka

Než začnete používat tyto informace a produkt, který podporují, přečtěte si informace, které uvádí “Poznámky” na stránce 675.

Toto vydání se vztahuje k verzi 9 vydání 2 produktu IBM® MQ a ke všem následujícím vydáním a modifikacím, dokud nebude v nových vydáních uvedeno jinak.

Když odešlete informace do IBM, udělíte společnosti IBM nevýlučné právo použít nebo distribuovat informace libovolným způsobem, který společnost považuje za odpovídající, bez vzniku jakýchkoliv závazků vůči vám.

Obsah

zabezpečeníIBM MQ

Zabezpečení je důležitým aspektem pro vývojáře aplikací IBM MQ i pro administrátory systému IBM MQ .

Aktualizace zabezpečení

Ujistěte se, že veškerý hardware a software uvnitř zabezpečené zóny a na pracovních stanicích obsluhy jsou v rámci svého životního cyklu podpory, byl proveden upgrade s povinnými aktualizacemi softwaru a byly okamžitě použity aktualizace zabezpečení.

Další informace o aktualizacích zabezpečení najdete v následujících tématech:

- Všechny platformy na adrese IBM Security Bulletins
- Zabezpečení a integrita systému APAR v systému z/OS na portáluIBM Z System Integrity.

přehled zabezpečení

Tato kolekce témat představuje koncepce zabezpečení produktu IBM MQ .

Koncepce a mechanizmy zabezpečení, které se vztahují na jakýkoli počítačový systém, jsou prezentovány jako první, po nich následuje diskuse o těchto bezpečnostních mechanismech, jak jsou implementovány v produktu IBM MQ.

Bezpečnostní koncepce a mechanismy

Tato kolekce témat popisuje aspekty zabezpečení, které je třeba vzít v úvahu při instalaci produktu IBM MQ .

Běžně přijímaná bezpečnostní opatření jsou následující:

- “Identifikace a ověřování” na stránce 6
- “Autorizace” na stránce 6
- “Auditování” na stránce 6
- “Důvěrnost” na stránce 7
- “Integrita dat” na stránce 7

Mechanismy zabezpečení jsou technické nástroje a techniky, které se používají k implementaci služeb zabezpečení. Určitý mechanizmus může fungovat sám nebo s jinými, aby poskytl určitou službu. Příklady běžných mechanismů zabezpečení jsou následující:

- “Šifrování” na stránce 7
- “Digesty zpráv a digitální podpisy” na stránce 9
- “digitální certifikáty” na stránce 9
- “infrastruktura veřejných klíčů (PKI)” na stránce 13

Plánujete-li implementaci produktu IBM MQ , zvažte, které bezpečnostní mechanismy vyžadují, abyste implementovali ty aspekty zabezpečení, které jsou pro vás důležité. Další informace o tom, co byste měli zvážit po přečtení těchto témat, najdete v tématu “Plánování bezpečnostních požadavků” na stránce 79.

Související pojmy

“Práce s protokolem SSL” na stránce 268
Tato témata uvádějí pokyny pro provádění jednotlivých úloh souvisejících s použitím TLS s produktem IBM MQ.

Související úlohy

Připojení dvou správců front pomocí protokolu TLS

Identifikace a ověřování

Identifikací je schopnost jednoznačně identifikovat uživatele systému nebo aplikace běžící v systému. *Ověření* je schopnost prokázat, že uživatel nebo aplikace je skutečně tím, kdo je osoba nebo to, co tato aplikace tvrdí.

Například uvažte uživatele, který se přihlašuje k systému zadáním ID uživatele a hesla. Systém používá ID uživatele k identifikaci uživatele. Systém ověřuje uživatele v době přihlášení tím, že kontroluje, zda je zadané heslo správné.

Neodmítání

Službu *non-repudiation* lze zobrazit jako rozšíření služby identifikace a ověření. Obecně platí, že se neodmítání použije, když jsou data přenášena elektronicky; například příkaz k nákupu nebo prodeji akcií makléře nebo příkaz k převodu peněžních prostředků z jednoho účtu do druhého.

Celkový cíl služby nepopiratelnosti je schopen prokázat, že konkrétní zpráva je přidružená k určitému jednotlivci.

Služba nepopiratelnosti může obsahovat více než jednu komponentu, přičemž každá komponenta poskytuje jinou funkci. Pokud odesilatel zprávy někdy odepře její odeslání, neodmítání služby s *důkazem o původu* mohou příjemci poskytnout nepopiratelné důkazy o tom, že zpráva byla odeslána touto konkrétní osobou. Pokud příjemce zprávy někdy odepře její přijetí, může odesilatel poskytnout neodmítání služby s *důkazem o doručení* nepopiratelné důkazy o tom, že zpráva byla přijata touto konkrétní osobou.

V praxi je důkazem s téměř 100% jistotou nebo nepopiratelným důkazem obtížný cíl. V reálném světě není nic plně zabezpečeno. Správa zabezpečení se více zabývá správou rizik na úroveň, která je přijatelná pro obchod. V takovém prostředí je realističtější očekávání neodmítání služby schopen poskytnout důkaz, který je přípustný a který podporuje váš případ u soudu.

Neodmítání je relevantní služba zabezpečení ochrany dat v prostředí IBM MQ , protože IBM MQ je prostředek pro elektronické přenášení dat. Můžete například požadovat souběžné důkazy o tom, že určitá zpráva byla odeslána nebo přijata aplikací asociovanou s určitou osobou.

IBM MQ s Advanced Message Security neposkytuje jako součást své základní funkce neodmítání služby. Tato dokumentace k produktu však obsahuje návrhy na to, jak můžete v prostředí IBM MQ poskytnout vlastní neodmítání služby, a to tak, že napíšete své vlastní ukončovací programy.

Související pojmy

“Identifikace a ověření v produktu IBM MQ” na stránce 20
V produktu IBM MQmůžete implementovat identifikaci a ověření pomocí informací o kontextu zprávy a vzájemného ověření.

Autorizace

Autorizace chrání kritické prostředky v systému omezením přístupu pouze k autorizovaným uživatelům a jejich aplikacím. Brání neautorizovanému použití prostředku nebo použití prostředku neoprávněným způsobem.

Související pojmy

“Autorizace v produktu IBM MQ” na stránce 20
Oprávnění můžete použít k omezení konkrétních jednotlivců nebo aplikací ve vašem prostředí produktu IBM MQ .

Auditování

Auditování je proces zaznamenávání a kontroly událostí za účelem zjištění, zda došlo k neočekávané nebo neautorizované aktivitě, nebo zda byl proveden pokus o provedení takové aktivity.

Další informace o tom, jak nastavit autorizaci, najdete v tématu “Plánování autorizace” na stránce 83 a přidružených dílčích tématech.

Související pojmy

“Auditování v IBM MQ” na stránce 21
IBM MQ může vydávat zprávy událostí k záznamu, že došlo k neobvyklé aktivitě.

Důvěrnost

Služba *confidentiality* chrání citlivé informace před neoprávněným zveřejněním.

Když jsou citlivá data uložena lokálně, mohou být dostatečné mechanismy řízení přístupu k ochraně před předpokladem, že data nelze přečíst, pokud k ní nelze přistoupit. Je-li vyžadována větší úroveň zabezpečení, mohou být data šifrována.

Šifrovat citlivá data při přenosu po komunikační síti, zejména v nezabezpečené síti, jako je například Internet. V síťovém prostředí nejsou mechanizmy řízení přístupu efektivní proti pokusům o zachycení dat, jako je například odposlouchávání.

Integrita dat

Služba *integrita dat* zjišťuje, zda došlo k neautorizované úpravě dat.

Existují dva způsoby, jak mohou být data pozměněna: náhodně, přes chyby hardwaru a přenosu, nebo kvůli záměrnému útoku. Mnoho hardwarových produktů a přenosových protokolů má mechanizmy pro detekování a opravu chyb hardwaru a přenosu. Účelem služby integrity dat je zjistit záměrný útok.

Služba integrity dat si klade za cíl pouze zjistit, zda byla data upravena. Neklade za cíl obnovit data do původního stavu, pokud byla upravena.

Mechanizmy řízení přístupu mohou přispívat k integritě dat, protože data nelze upravit, pokud je přístup odepřen. Avšak, stejně jako v případě utajení, mechanismy řízení přístupu nejsou účinné v prostředí sítě.

Koncepce šifrování

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

Výraz *entita* se používá k odkazování na správce front, IBM MQ MQI client, individuálního uživatele nebo jakýkoli jiný systém schopný vyměňovat si zprávy.

Související pojmy

“Šifrování v produktu IBM MQ” na stránce 22
Produkt IBM MQ poskytuje šifrování pomocí protokolu TLS (Transport Security Layer).

Šifrování

Šifrování je proces převedení mezi čitelným textem, který se nazývá *prostý text*, a nečitelným formulářem s názvem *šifrovaný text*.

K tomu dojde následujícím způsobem:

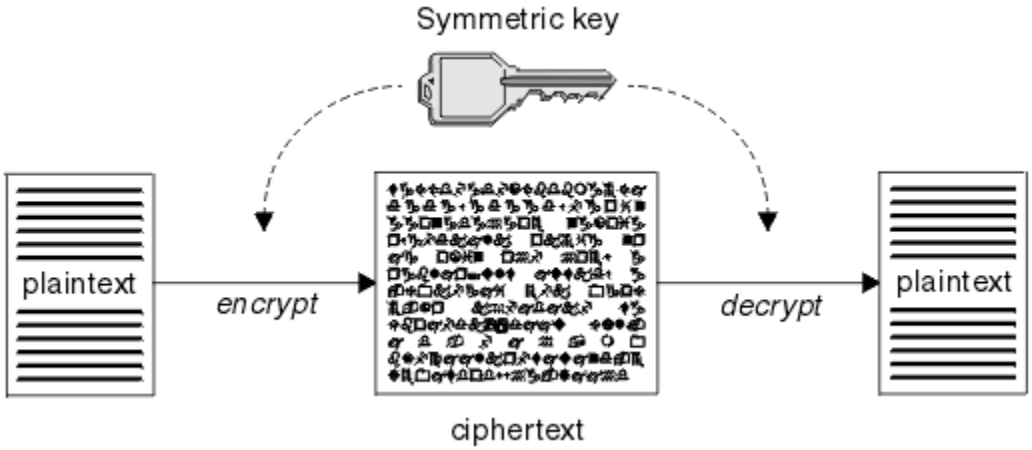
1. Odesílatel převádí zprávu prostého textu na šifrovaný text. Tato část procesu se nazývá *šifrování* (někdy *encipherment*).
2. Šifrovací text se přenáší do přijímače.
3. Příjemce převádí zprávu šifrovaného textu zpět na její prostý textový tvar. Tato část procesu se nazývá *dešifrování* (někdy *dešifrovací*).

Převod zahrnuje posloupnost matematických operací, které mění vzhled zprávy během přenosu, ale nemají vliv na obsah. Kryptografické techniky mohou zajistit důvěrnost a ochranu zpráv proti neoprávněnému prohlížení (odposlouchávání), protože šifrovaná zpráva není srozumitelná. Digitální podpisy, které poskytují záruku integrity zpráv, používají šifrovací techniky. Další informace viz “Digitální podpisy v SSL/TLS” na stránce 18.

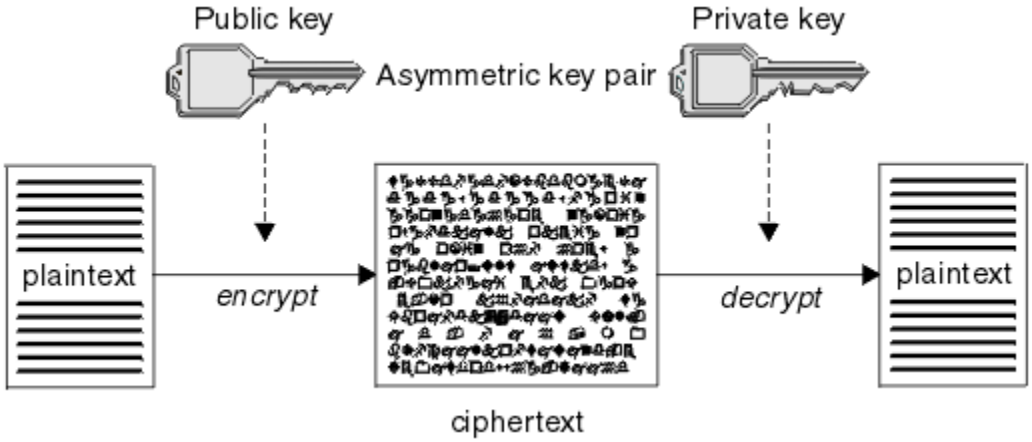
Kryptografické techniky zahrnují obecný algoritmus, který je specifický pro použití klíčů. Existují dvě třídy algoritmu:

- Ty, které požadují, aby obě strany používaly stejný tajný klíč. Algoritmy, které používají sdílený klíč, jsou známé jako *symetrické* algoritmy. Obrázek 1 na stránce 8 ilustruje šifrování pomocí symetrických klíčů.
- Ty, které používají jeden klíč k šifrování a jiný klíč pro dešifrování. Jeden z nich musí být tajemný, ale druhý může být veřejný. Algoritmy, které používají páry veřejného a soukromého klíče, jsou známy jako *asymetrické* algoritmy. Obrázek 2 na stránce 8 ilustruje asymetrické šifrování kláves, které se také nazývá *šifrování pomocí veřejného klíče*.

Použité algoritmy šifrování a dešifrování mohou být veřejné, ale sdílený tajný klíč a soukromý klíč musí být uchovány v tajnosti.



Obrázek 1. šifrování pomocí symetrických klíčů



Obrázek 2. šifrování pomocí asymetrických klíčů

Obrázek 2 na stránce 8 uvádí prostý text zašifrovaný pomocí veřejného klíče příjemce a dešifrován pomocí soukromého klíče příjemce. Soukromý klíč pro dešifrování šifrovaného textu obsahuje pouze určený příjemce. Všimněte si, že odesilatel může také šifrovat zprávy pomocí soukromého klíče, což umožňuje komukoli, kdo zadržuje veřejný klíč odesílatele, dešifrovat zprávu a ujistit se, že zpráva musí pocházet od odesílatele.

Při použití asymetrických algoritmů jsou zprávy šifrovány buď s veřejným, nebo soukromým klíčem, ale lze je dešifrovat pouze pomocí druhého klíče. Pouze soukromý klíč je tajný, veřejný klíč může být znám kdokoli. Se symetrickým algoritmem musí být nasdílený klíč znám pouze oběma stranám. Tomu se říká *problém s distribucí klíčů*. Asymetrické algoritmy jsou pomalejší, ale mají tu výhodu, že se nevyskytne žádný problém s distribucí klíče.

Další terminologie spojená se šifrováním je:

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

1024 bitů	Nízkostý asymetrický klíč
2048 bitů	Asymetrický klíč střední síly
4096 bitů	Vysoce odolný asymetrický klíč

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

Algoritmus blokového šifrování
Tyto algoritmy šifrují data po blocích. Například, algoritmus RC2 z RSA Data Security Inc. používá bloky 8 bajtů dlouhý. Blokové algoritmy jsou obvykle pomalejší než proudové algoritmy.

Algoritmus šifry proudu
Tyto algoritmy fungují na každém bajtu dat. Algoritmy proudů jsou obvykle rychlejší než blokové algoritmy.

Digesty zpráv a digitální podpisy
Kód digest zprávy je číselným znázorněním pevné velikosti obsahu zprávy. Kód digest zprávy je počítán pomocí hašovací funkce a lze jej zašifrovat, čímž se vytvoří digitální podpis.

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

- Musí to být jedna cesta. Aby bylo možno nalézt zprávu odpovídající konkrétnímu kódu digest zprávy jiným způsobem než testováním všech možných zpráv, nesmí být možné tuto funkci vrátit zpět.
- Pro nalezení dvou zpráv, které mají hašování na stejný kód digest, musí být výpočty dvou zpráv neúměrně dosažitelné.

Kód digest zprávy se odešle se zprávou samotnou. Příjemce může vygenerovat kód digest pro zprávu a porovnat jej s použitím kódu digest odesilatele. Integrita zprávy je ověřena, jsou-li dvě shrnutí zpráv stejná. Jakákoli manipulace se zprávou během přenosu téměř jistě má za následek jiný kód digest zprávy.

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

Odesílatel může také vygenerovat kód digest zprávy a poté šifrovat kód digest pomocí soukromého klíče asymetrického páru klíčů a vytvořit tak digitální podpis. Podpis musí být poté dešifrován příjemcem, než jej porovnáte s lokálně generovaným kódem digest.

Související pojmy
“Digitální podpisy v SSL/TLS” na stránce 18
Digitální podpis je vytvořen šifrováním reprezentace zprávy. Šifrování používá soukromý klíč podepsané osoby a v zájmu efektivity obvykle pracuje na kódu digest zprávy spíše než na samotném zprávě.

digitální certifikáty
Digitální certifikáty chrání před ztělesněním a potvrzují, že veřejný klíč patří do zadané entity. Vydávají je certifikační autorita.

Digitální certifikáty poskytují ochranu proti ztělesnění, protože digitální certifikát váže veřejný klíč ke svému vlastníkovi, ať je tento vlastník jednotlivec, správce front nebo jiná entita. Digitální certifikáty jsou také známé jako certifikáty veřejných klíčů, protože vám poskytují záruky ohledně vlastnictví veřejného klíče, používáte-li asymetrický systém klíčů. Digitální certifikát obsahuje veřejný klíč pro entitu a je to prohlášení, že veřejný klíč patří do této entity:

- Je-li certifikát určen pro jednotlivou entitu, je certifikát označován jako *osobní certifikát* nebo *uživatelský certifikát*.
- Je-li certifikát pro certifikační autoritu, certifikát se nazývá *certifikát CA* nebo *certifikát podepsaného*.

Pokud jsou veřejné klíče odeslány přímo jejich vlastníkem do jiné entity, je zde riziko, že zpráva bude zachycena a veřejný klíč nahradí jiným. Tento stav je znám jako *muž uprostřed útoku*. Řešením tohoto problému je výměna veřejných klíčů prostřednictvím důvěryhodné třetí strany, což vám dává silné ujištění, že veřejný klíč skutečně patří k subjektu, s nímž komunikujete. Místo přímého odeslání svého veřejného

klíče se obraťte na důvěryhodnou třetí stranu, aby ji začlenila do digitálního certifikátu. Důvěryhodná třetí strana, která vydává digitální certifikáty, se nazývá certifikační autorita (CA), jak je popsáno v "Vydavatelé certifikátů" na stránce 10.

Co je v digitálním certifikátu
Digitální certifikáty obsahují specifické části informací určené standardem X.509 .

Digitální certifikáty používané produktem IBM MQ vyhovují standardu X.509 , který určuje požadované informace a formát pro jejich odeslání. X.509 je část rámce ověření řady standardů X.500 .

Digitální certifikáty obsahují alespoň následující informace o certifikovaném subjektu:

- Veřejný klíč vlastníka
- Rozlišující název vlastníka
- Rozlišovací jméno certifikační autority, která vydala certifikát
- Datum, od kterého je certifikát platný
- Datum ukončení platnosti certifikátu
- Číslo verze datového formátu certifikátu, jak je definováno v X.509. Aktuální verze standardu X.509 je verze 3 a většina certifikátů je v souladu s touto verzí.
- 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 dvě certifikáty podepsané stejným certifikátem CA nemají stejné sériové číslo.

Certifikát X.509 verze 2 také obsahuje identifikátor vydavatele a identifikátor subjektu a certifikát X.509 verze 3 může obsahovat několik rozšíření. Některá rozšíření certifikátu, jako je například rozšíření Základní omezení, jsou *standard*, ale jiné jsou specifické pro implementaci. Rozšíření může být *kritické*, v takovém případě musí být systém schopen pole rozpoznat; pokud pole nerozpozná, musí tento certifikát odmítnout. Pokud rozšíření není kritické, může systém ignorovat, pokud jej nerozpozná.

Digitální podpis v osobním certifikátu je generován pomocí soukromého klíče CA, který tento certifikát podepsal. Každý, kdo potřebuje ověřit osobní certifikát, může použít veřejný klíč CA k tomu, aby tak mohl učinit. Certifikát CA obsahuje svůj veřejný klíč.

Digitální certifikáty neobsahují váš soukromý klíč. Musíte zachovat své soukromé tajné klíče.

Požadavky na osobní certifikáty
Produkt IBM MQ podporuje digitální certifikáty, které splňují požadavky standardu X.509 . Vyžaduje volbu ověření klienta.

Protože IBM MQ je peer k rovnocennému systému, je v terminologii SSL/TLS zobrazen jako ověření klienta. Proto musí osobní certifikát použitý pro ověření SSL/TLS umožňovat použití klíče ověření klienta. Ne všechny serverové certifikáty mají tuto volbu povoleny, takže poskytovatel certifikátu možná bude muset povolit ověření klienta na kořenové CA pro zabezpečený certifikát.

Kromě standardů, které specifikují formát dat pro digitální certifikát, existují také standardy pro určení, zda je certifikát platný. Tyto standardy byly aktualizovány v průběhu času, aby se zabránilo určitým typům narušení zabezpečení. Například starší certifikáty X.509 verze 1 a 2 neoznačovaly, zda by certifikát mohl být legitimně použit k podepsání jiných certifikátů. Bylo proto možné, aby zlomyslný uživatel získal osobní certifikát z legitimního zdroje a vytvořil nové certifikáty určené k napodobení ostatních uživatelů.

Při použití certifikátů X.509 verze 3 se používají rozšíření certifikátů BasicConstraints a KeyUsage k určení, které certifikáty mohou legitimně podepisovat jiné certifikáty. Standard IETF RFC 5280 uvádí řadu pravidel pro ověření platnosti certifikátu, které musí implementovat vyhovující aplikační software, aby se zabránilo útokům zosobnění. Sada pravidel certifikátu je známá jako zásada ověření platnosti certifikátu.

Další informace o zásadách ověření platnosti certifikátů v produktu IBM MQnaleznete v tématu "Zásady ověření platnosti certifikátu v produktu IBM MQ" na stránce 42.

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

Role CA jsou:

- Při přijetí požadavku na digitální certifikát ověřit identitu žadatele před sestavením, podepsáním a vrácením osobního certifikátu
- Zajištění vlastního veřejného klíče vydavatele certifikátů ve svém certifikátu CA
- Chcete-li publikovat seznamy certifikátů, které již nejsou důvěryhodné v seznamu odvolaných certifikátů (CRL). Další informace naleznete v tématu “Práce se zrušenými certifikáty” na stránce 330
- Zajištění přístupu k stavu odvolání certifikátu pomocí fungování serveru odpovídacího modulu OCSP

Rozlišující názvy
Rozlišující název (Distinguished Name-DN) jedinečně identifikuje entitu v certifikátu X.509 .

Upozornění: Ve filtru SSLPEER mohou být použity pouze atributy uvedené v následující tabulce. DN certifikátů mohou obsahovat jiné atributy, ale filtrování není na těchto atributech povoleno.

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

Typ atributu	**Popis**
SERIALNUMBER	Sériové číslo certifikátu
MAIL	E-mailová adresa
E	E-mailová adresa (zamítnuto ve prospěch volby MAIL)
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
PC	PSČ
C	Země
UNSTRUCTUREDNAME	Název hostitele
UNSTRUCTUREDADDRESS	Adresa IP
DNQ	Kvalifikátor rozlišujícího názvu

Standard X.509 definuje další atributy, které obvykle netvoří část rozlišujícího názvu, ale mohou poskytnout nepovinná rozšíření digitálního certifikátu.

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

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

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

DN může obsahovat více atributů OU a DC. Povolena je pouze jedna instance každého z ostatních atributů. Pořadí položek organizačních jednotek je důležité: pořadí určuje hierarchii názvů organizační jednotky, přičemž nejprve se použije jednotka highest-level. Pořadí záznamů DC je také významné.

IBM MQ toleruje určité poškozené DN. Další informace viz IBM MQ pravidla pro hodnoty SSLPEER.

Související pojmy

“Co je v digitálním certifikátu” na stránce 10
Digitální certifikáty obsahují specifické části informací určené standardem X.509 .

Získání osobních certifikátů z certifikační autority
Certifikát můžete získat od důvěryhodné externí certifikační autority (CA).

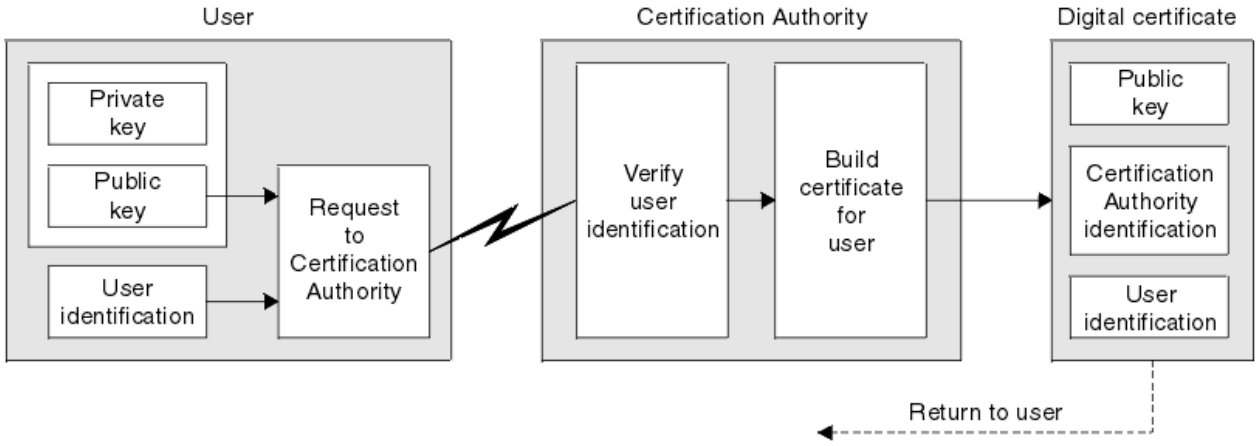
Digitální certifikát získáte odesláním informací do CA ve formě žádosti o certifikát. Standard X.509 definuje formát pro tyto informace, ale některé CA mají svůj vlastní formát. Požadavky na certifikáty jsou typicky generovány nástrojem pro správu certifikátů, který váš systém používá; například:

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

Informace obsahují váš rozlišující název a váš veřejný klíč. Když nástroj pro správu certifikátů vygeneruje žádost o certifikát, vygeneruje také Váš soukromý klíč, který musíte udržovat v bezpečí. Nikdy nerozdělte svůj soukromý klíč.

Když certifikační autorita obdrží váš požadavek, ověří vaši identitu před sestavením certifikátu a vrátí vám to jako osobní certifikát.

Obrázek 3 na stránce 12 ilustruje proces získání digitálního certifikátu od CA.



Obrázek 3. Získání digitálního certifikátu

V diagramu:

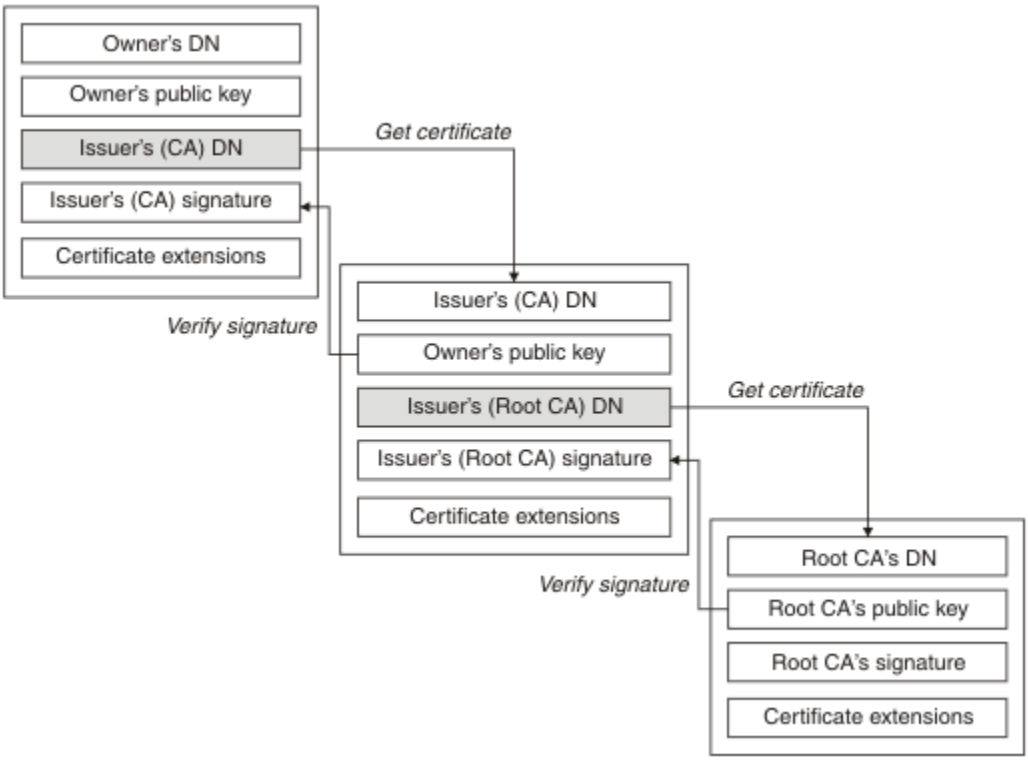
- Identifikace uživatele zahrnuje váš rozlišující název předmětu.
- Identifikace certifikačního orgánu zahrnuje rozlišovací jméno CA, který vydává tento certifikát.

Digitální certifikáty obsahují jiná pole než ta, která jsou uvedena v diagramu. Další informace o ostatních polích v digitálním certifikátu viz “Co je v digitálním certifikátu” na stránce 10.

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

Řetězec certifikátu, také známý jako *cesta certifikace*, je seznam certifikátů použitých k ověření identity entity. Řetěz 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 sám certifikační autoritou (CA). Podpisy všech certifikátů v řetězci musí být ověřeny, dokud nebude dosaženo kořenového certifikátu CA.

Obrázek 4 na stránce 13 ilustruje certifikační cestu od vlastníka certifikátu k kořenové CA, kde začíná řetězec důvěry.



Obrázek 4. Linie důvěry

Každý certifikát může obsahovat jedno nebo více rozšíření. Certifikát patřící CA obvykle obsahuje rozšíření BasicConstraints s nastavením příznaku isCA , aby označilo, že je povoleno podepisovat jiné certifikáty.

Když certifikáty již nejsou platné
Digitální certifikáty mohou vypršet nebo zrušit jejich platnost.

Digitální certifikáty jsou vydávány na pevné období a nejsou platné po datu jejich použitelnosti.

Certifikáty mohou být odvolány z různých důvodů včetně:

- Vlastník byl přesunut do jiné organizace.
- Soukromý klíč již není žádným tajemstvím.

Produkt IBM MQ může zkontrolovat, zda je certifikát odvolán odesláním požadavku na odpovídací modul protokolu OCSP (Online Certificate Status Protocol) (pouze na serveru AIX, Linux, and Windows). Případně mohou mít přístup k seznamu odvolaných certifikátů (CRL) na serveru LDAP. Informace o odvolání OCSP a CRL jsou publikovány vydavatelem certifikátů. Další informace viz “Práce se zrušenými certifikáty” na stránce 330.

infrastruktura veřejných klíčů (PKI)

PKI (Public Key Infrastructure) je systém zařízení, zásad a služeb, které podporují použití šifrování pomocí veřejného klíče pro ověření stran účastnících se transakce.

Neexistuje jediný standard, který definuje komponenty infrastruktury veřejného klíče, ale PKI obvykle obsahuje certifikační autority (CA) a registrační autority (Ras). Certifikační autority poskytují následující služby:

- Vydávání digitálních certifikátů
- Ověření digitálních certifikátů
- Zrušení platnosti digitálních certifikátů

- Distribuce veřejných klíčů

Standardy X.509 poskytují základ pro odvětvovou infrastrukturu Public Key Infrastructure.

Další informace o digitálních certifikátech a certifikačních autorech (CA) naleznete v příručce “digitální certifikáty” na stránce 9 . Ověření Ras ověřuje informace poskytnuté při požadavku na digitální certifikáty. Pokud RA tyto informace ověří, může CA vydat digitální certifikát žadateli.

PKI může také poskytovat nástroje pro správu digitálních certifikátů a veřejných klíčů. PKI je někdy popisována jako *hierarchie důvěryhodnosti* pro správu digitálních certifikátů, ale většina definic zahrnuje i další služby. Některé definice zahrnují služby šifrování a digitálních podpisů, ale tyto služby nejsou nezbytně nutné pro provoz PKI.

Kryptografické bezpečnostní protokoly: TLS

Kryptografické protokoly zajišťují zabezpečená spojení, což umožňuje dvěma stranám komunikovat s ochranou soukromí a integrity dat. Protokol Transport Layer Security (TLS) se vyvinul z zabezpečení SSL (Secure Sockets Layer). IBM MQ podporuje TLS.

Primárními cíli obou protokolů je poskytovat utajení (někdy označované jako *soukromí*), integritu dat, identifikaci a autentizaci pomocí digitálních certifikátů.

Ačkoli jsou tyto dva protokoly podobné, rozdíly jsou dostatečně významné, že SSL 3.0 a různé verze TLS nespolupracují.

Související pojmy

“Protokoly zabezpečení TLS v produktu IBM MQ” na stránce 22
Produkt IBM MQ podporuje protokol TLS (Transport Layer Security) k poskytování zabezpečení na úrovni odkazů pro kanály zpráv a kanály MQI.

Koncepce zabezpečení přenosové vrstvy (TLS)

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

Protokol TLS poskytuje komunikační zabezpečení přes internet a umožňuje aplikacím typu klient/server komunikovat způsobem, který je důvěrný a spolehlivý. Protokoly mají dvě vrstvy: protokol záznamu a protokol navázání komunikace, které jsou vrstvovány nad přenosovým protokolem, jako např. TCP/IP. Oba používají asymetrické a symetrické kryptografické techniky.

Připojení TLS je inicializováno 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 CipherSpecs podporovaných produktem IBM MQ je k dispozici na adrese “Povolení CipherSpecs” na stránce 408.

Další informace o protokolu SSL naleznete v informacích poskytnutých na adrese https://developer.mozilla.org/docs/Mozilla/Projects/NSS. Další informace o protokolu TLS naleznete v informacích, které poskytuje pracovní skupina TLS na webovém serveru jednotky Internet Engineering Task Force na adrese https://www.ietf.org

Přehled navázání komunikace SSL/TLS

Předávání řídicích signálů SSL/TLS umožňuje klientu TLS a serveru ustanovit tajné klíče, se kterými komunikují.

Tato část obsahuje souhrn kroků, které umožňují komunikaci klienta a serveru TLS spolu s ostatními.

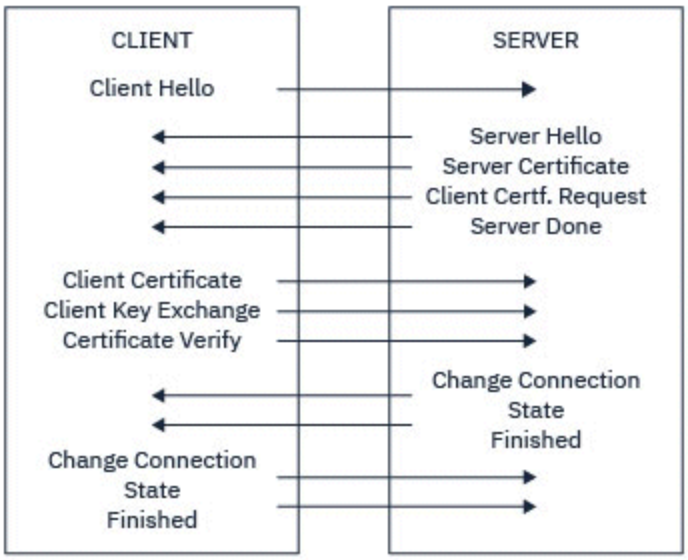
- Shodněte se na verzi protokolu, který se má použít.
- Vyberte šifrovací algoritmy.
- Proveďte vzájemnou autentizaci tím, že si vyměníte a ověřujete digitální certifikáty.
- Použijte asymetrické šifrovací techniky ke generování sdíleného tajného klíče, který se vyvaruje problému s distribucí klíčů. TLS pak používá sdílený klíč pro symetrické šifrování zpráv, které je rychlejší než asymetrické šifrování.

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

V přehledu jsou kroky zapojené do navázání komunikace TLS následující:

1. Klient TLS odešle zprávu "client hello" , která vypisuje šifrovací informace, jako je verze TLS, a v pořadí klienta dle předvoleb klienta CipherSuites podporované klientem. Zpráva také obsahuje náhodný bajtový řetězec, který se používá při následných výpočtech. Protokol umožňuje, aby "hello klienta" obsahovalo metody komprese dat podporované klientem.
2. Server TLS odpoví zprávou "server hello" , která obsahuje sadu CipherSuite vybranou serverem ze seznamu poskytovaného klientem, ID relace a dalším náhodným bajtovým řetězcem. Server také odesílá svůj digitální certifikát. Pokud server vyžaduje digitální certifikát pro ověření klienta, odešle server "požadavek na certifikát klienta" , který obsahuje seznam podporovaných typů certifikátů a rozlišující názvy přijatelných certifikačních autorit (CA).
3. Klient TLS ověřuje digitální certifikát serveru. Další informace viz “Jak TLS poskytuje identifikaci, autentizaci, důvěrnost a integritu” na stránce 16.
4. Klient TLS odešle náhodný bajtový řetězec, který umožňuje klientovi i serveru vypočítat tajný klíč, který se má použít pro šifrování následných dat zprávy. Samotný náhodný bajtový řetězec je zašifrován pomocí veřejného klíče serveru.
5. Pokud server TLS odeslal "požadavek na certifikát klienta", odešle klient náhodný bajtový řetězec zašifrovaný pomocí soukromého klíče klienta, spolu s digitálním certifikátem klienta, nebo "bez výstrahy digitálního certifikátu". Tato výstraha je pouze varováním, ale s některými implementacemi se navázání komunikace nezdaří, je-li ověřování klienta povinné.
6. Server TLS ověřuje certifikát klienta. Další informace viz “Jak TLS poskytuje identifikaci, autentizaci, důvěrnost a integritu” na stránce 16.
7. Klient TLS odešle serveru zprávu "finished" , která je zašifrována pomocí tajného klíče označující, že je část klienta navázání komunikace dokončena.
8. Server TLS odešle klientovi zprávu "finished" , která je zašifrována pomocí tajného klíče, což indikuje, že část serveru handshake je dokončena.
9. Po dobu trvání relace TLS může server a klient nyní vyměňovat zprávy, které jsou symetricky šifrovány pomocí sdíleného tajného klíče.

Obrázek 5 na stránce 15 ilustruje navázání komunikace TLS.



Obrázek 5. Přehled navázání komunikace TLS

Jak TLS poskytuje identifikaci, autentizaci, důvěrnost a integritu

Během ověření klienta i serveru je nutný krok, který vyžaduje zašifrování dat s jedním z klíčů v asymetrickém páru klíčů a dešifrován s druhým klíčem dvojice. Kód digest zprávy se používá k zajištění integrity.

Přehled kroků souvisejících s výměnou potvrzení TLS naleznete v tématu “Přehled navázání komunikace SSL/TLS” na stránce 14.

Jak TLS poskytuje ověření

Pro ověření serveru klient používá veřejný klíč serveru k zašifrování dat, která se používají k výpočtu tajného klíče. Server může generovat tajný klíč pouze tehdy, může-li dešifrovat data se správným soukromým klíčem. Samotný náhodný bajtový řetězec je zašifrován pomocí veřejného klíče serveru (krok “4” na stránce 15 v přehledu).

Pro ověření klienta používá server veřejný klíč v certifikátu klienta k dešifrování dat, která klient odešle během kroku “5” na stránce 15 navázání komunikace. Výměna dokončených zpráv, které jsou šifrovány pomocí tajného klíče (kroky “7” na stránce 15 a “8” na stránce 15 v přehledu) potvrdí, že ověření je dokončeno.

Pokud některý z kroků ověření selže, 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 proti ztělesnění, najdete v souvisejících informacích. Požadované certifikáty jsou následující, kde CA X vydává certifikát pro klienta TLS a CA Y vydává certifikát na server TLS:

Pouze pro ověření serveru vyžaduje server TLS:

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

a potřeby klienta TLS:

- Certifikát CA pro CA Y

Pokud server TLS vyžaduje autentizaci klienta, server ověřuje identitu klienta ověřením digitálního certifikátu klienta s veřejným klíčem pro CA, který vydal osobní certifikát klientovi, v tomto případě CA X. Pro autentizaci serveru i klienta vyžaduje server:

- Osobní certifikát vydaný na server certifikační autoritou Y
- Soukromý klíč serveru
- Certifikát CA pro CA X

a potřeby klienta:

- Osobní certifikát vydaný pro klienta certifikační autoritou X
- Soukromý klíč klienta
- Certifikát CA pro CA Y

Jak server TLS, tak klient mohou potřebovat další certifikáty CA pro vytvoření řetězce certifikátů do kořenového certifikátu CA. Další informace o řetězcích certifikátů naleznete v souvisejících informacích.

Co se děje během ověření certifikátu

Jak je uvedeno v krocích “3” na stránce 15 a “6” na stránce 15 v přehledu, klient TLS ověřuje certifikát serveru a server TLS ověřuje certifikát klienta. K tomuto ověření jsou čtyři aspekty:

1. Digitální podpis je zkontrolován (viz “Digitální podpisy v SSL/TLS” na stránce 18).
2. Řetěz certifikátů je zaškrtnut; měli byste mít intermediační certifikáty CA (viz “Způsob práce řetězů certifikátů” na stránce 12).
3. Jsou zkontrolována data vypršení platnosti a aktivace a období platnosti.

4. Stav odvolání certifikátu je zkontrolován (viz “Práce se zrušenými certifikáty” na stránce 330).

Reset tajného klíče

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

Tajný klíč je generován z náhodného textu odeslaného jako část 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 změněna. Další informace viz “Digesty zpráv a digitální podpisy” na stránce 9.

Pokud je odhalen tajný klíč, může být šifrovaný text zprávy dešifrován od šifrovaného textu nebo by bylo možné vypočítat shrnutí zprávy, které umožňuje změnu zpráv bez detekce. Dokonce i pro komplexní algoritmus, může být konečně objevený prostý text tím, že uplatní všechny možné matematické transformace na šifrovaný text. Chcete-li minimalizovat množství dat, které lze dešifrovat nebo změnit, je-li tajný klíč porušen, může být tajný klíč pravidelně znovu dohodnutý. Když je tajný klíč znovu vyjednán, předchozí tajný klíč již nemůže být použit k dešifrování dat šifrovaných pomocí nového tajného klíče.

Jak TLS poskytuje utajení

TLS používá kombinaci symetrického a asymetrického šifrování k zajištění ochrany soukromí zpráv. Při navázání komunikace TLS se klient a server TLS dohodnou šifrovací algoritmus a sdílený tajný klíč, který má být použit 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 v případě, že je zachycena. Protože TLS používá při přenášení sdíleného tajného klíče asymetrické šifrování, neexistuje žádný problém s distribucí klíče. Další informace o technikách šifrování naleznete v tématu “Šifrování” na stránce 7.

Jak TLS poskytuje integritu

TLS poskytuje integritu dat vypočtením kódu digest zprávy. Další informace jsou uvedeny v tématu “Integrita dat zpráv” na stránce 465.

Použití TLS zajišťuje integritu dat, za předpokladu, že CipherSpec ve vaší definici kanálu používá hašovací algoritmus popsaný v tabulce v produktu “Povolení CipherSpecs” na stránce 408.

Zejména platí, že pokud se týká integrity dat, měli byste se vyhnout výběru CipherSpec , jejíž hašovací algoritmus je uveden jako "Žádný". Použití MD5 je také silně nedoporučováno, protože je nyní velmi staré a již není bezpečné pro většinu praktických účelů.

CipherSpecs a CipherSuites

Kryptografické bezpečnostní protokoly musí souhlasit s algoritmem používaným zabezpečeným připojením. CipherSpecs a CipherSuites definují specifické kombinace algoritmů.

CipherSpec identifikuje kombinaci šifrovacího algoritmu a algoritmu pro ověřování zpráv (MAC). Oba konce připojení TLS se musí dohodnout na stejné sadě CipherSpec , aby mohly komunikovat.

Produkt IBM MQ podporuje protokoly TLS1.3 a TLS1.2 a CipherSpecs. Můžete však povolit zamítnutý CipherSpecs, pokud to potřebujete.

Informace o následujících tématech viz “Povolení CipherSpecs” na stránce 408 :

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

Důležité: Při práci s kanály produktu IBM MQ se používá CipherSpec. Při práci s kanály produktu Java , kanály produktu JMS nebo kanály MQTT určujete volbu CipherSuite.

Další informace o CipherSpecsviz “Povolení CipherSpecs” na stránce 408.

Sada CipherSuite je sada šifrovacích algoritmů používaných připojením TLS. Sada obsahuje tři různé algoritmy:

- Algoritmus výměny klíčů a ověření, použitý 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 některé kombinace jsou platné, jsou-li zadány pro připojení TLS. Název platné CipherSuite definuje kombinaci použitých algoritmů. Příklad: Hodnota CipherSuite TLS_RSA_WITH_AES_128_CBC_SHA určuje následující volby:

- Směnný a ověřovací algoritmus RSA
- Šifrovací algoritmus AES používající 128bitový klíč a režim CBC (cipher block chaining).
- Autentizační kód zprávy SHA-1 (MAC)

Digitální podpisy v SSL/TLS

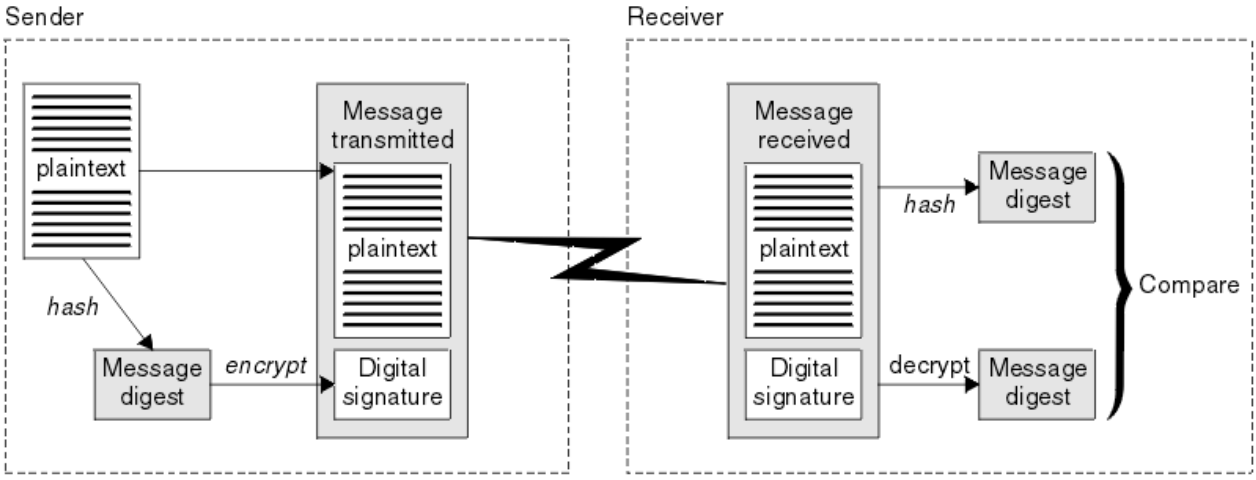
Digitální podpis je vytvořen šifrováním reprezentace zprávy. Šifrování používá soukromý klíč podepsané osoby a v zájmu efektivity obvykle pracuje na kódu digest zprávy spíše než na samotném zprávě.

Digitální podpisy se liší od podepisovaných dat, na rozdíl od rukou psaných podpisů, které nezávisí na obsahu podepsaného dokumentu. Jsou-li dvě různé zprávy podepsány digitálně stejnou entitou, tyto dva podpisy se liší, ale oba podpisy lze ověřit se stejným veřejným klíčem, tj. veřejným klíčem entity, která podepsala zprávy.

Postup digitálního podpisu je následující:

1. Odesilatel vypočítá shrnutí zprávy a poté šifruje kód digest pomocí soukromého klíče odesílatele a vytváří digitální podpis.
2. Odesílatel přenáší digitální podpis se zprávou.
3. Příjemce dešifruje digitální podpis pomocí veřejného klíče odesílatele a regeneruje kód digest zprávy odesilatele.
4. Příjemce vypočítá kód digest zprávy z přijatých dat zprávy a ověří, zda jsou dva moduly digest stejné.

Tento proces ilustruje produkt Obrázek 6 na stránce 18 .



Obrázek 6. Proces digitálního podpisu

Je-li digitální podpis ověřen, příjemce ví, že:

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

Digitální podpisy jsou součástí integrity a ověřovacích služeb. Digitální podpisy také poskytují důkaz o původu. Pouze odesilatel zná soukromý klíč, který poskytuje pádné 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" . Certifikát pro tento modul byl přesunut do historického stavu. Zákazníci by si měli prohlédnout IBM Crypto for C certificate a měli by si být vědomi jakýchkoli 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 19
Vláda Spojených států amerických vyrábí technické poradenství v oblasti IT systémů a zabezpečení, včetně šifrování dat. Národní bezpečnostní agentura USA (NSA) doporučuje soubor interoperabilních šifrovacích algoritmů ve standardu Suite B.

Národní bezpečnostní agentura (NSA) Suite B Kryptografie

Vláda Spojených států amerických vyrábí technické poradenství v oblasti IT systémů a zabezpečení, včetně šifrování dat. Národní bezpečnostní agentura USA (NSA) doporučuje soubor interoperabilních šifrovacích algoritmů ve standardu Suite B.

Standard Suite B určuje provozní režim, ve kterém jsou použity pouze specifické sady zabezpečovacích šifrovacích algoritmů. Standard Suite B uvádí:

- Šifrovací algoritmus (AES)
- Algoritmus výměny klíčů (Elliptic Curve Diffie-Hellman, také známý jako ECDH)
- Algoritmus digitálního podpisu (algoritmus digitálního podpisu Elliptic Curve, také známý jako ECDSA)
- Algoritmy hašování (SHA-256 nebo SHA-384)

Kromě toho standard IETF RFC 6460 uvádí profily vyhovující standardu Suite B, které definují podrobnou konfiguraci aplikace a chování nezbytné k dosažení souladu se standardem Suite B. Definuje dva profily:

1. Profil vyhovující standardu Suite B pro použití s TLS 1.2. Je-li konfigurována pro kompatibilní operaci Suite B, použije se pouze omezená sada šifrovacích algoritmů.
2. Přechodný profil pro použití s TLS 1.0 nebo TLS 1.1. Tento profil umožňuje interoperabilitu se servery, které nevyhovují standardu Suite B. Je-li konfigurována pro přechodnou operaci Suite B, mohou být použity další algoritmy šifrování a hašování.

Standard Suite B je koncepčně podobný standardu FIPS 140-2, protože omezuje sadu povolených šifrovacích algoritmů tak, aby byla zajištěna zajištěná úroveň zabezpečení.

Na systémech AIX, Linux, and Windows lze IBM MQnakonfigurovat tak, aby vyhovovalo profilu TLS 1.2 standardu Suite B, ale přechodný profil sady Suite B nepodporuje. Další informace uvádí téma “Šifrování NSA Suite B v IBM MQ” na stránce 39.

Související odkazy

“Federální standardy zpracování informací” na stránce 19

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 vysvětluje, jak můžete implementovat různé koncepce zabezpečení v produktu IBM MQ.

Produkt IBM MQ poskytuje mechanizmy pro implementaci všech koncepcí zabezpečení uvedených v produktu “Bezpečnostní koncepce a mechanismy” na stránce 5. O těchto tématech se podrobněji pojednává v následujících sekcích.

Identifikace a ověření v produktu IBM MQ

V produktu IBM MQmůžete implementovat identifikaci a ověření pomocí informací o kontextu zprávy a vzájemného ověření.

Zde je několik příkladů identifikace a ověření v prostředí produktu IBM MQ :

- Každá zpráva může obsahovat informace *kontext zprávy* . Tyto informace jsou uloženy v deskriptoru zpráv. Může být generovaný správcem front, když je zpráva vložena do fronty aplikací. Alternativně může aplikace dodat informace, pokud je ID uživatele přidružené k aplikaci autorizováno k provedení.

  Informace o kontextu ve zprávě umožňují přijímající aplikaci zjistit informace o odesílateli zprávy. Obsahuje například název aplikace, která vložila tuto zprávu, a ID uživatele přidružené k aplikaci.
- Když se spustí kanál zpráv, je možné, aby byl agent kanálu zpráv (MCA) na každém konci kanálu autentizoval jeho partnera. Tato technika je známá jako *vzájemné ověření*. Pro odesílajícího agenta MCA poskytuje ujištění, že partner, o který se chystá odeslat zprávy, je původní. Pro přijímajícího agenta MCA existuje podobné ujištění o tom, že se chystá přijímat zprávy od skutečného partnera.

Související pojmy

“Identifikace a ověřování” na stránce 6
Identifikací je schopnost jednoznačně identifikovat uživatele systému nebo aplikace běžící v systému. *Ověření* je schopnost prokázat, že uživatel nebo aplikace je skutečně tím, kdo je osoba nebo to, co tato aplikace tvrdí.

Autorizace v produktu IBM MQ

Oprávnění můžete použít k omezení konkrétních jednotlivců nebo aplikací ve vašem prostředí produktu IBM MQ .

Zde je několik příkladů autorizace v prostředí produktu IBM MQ :

- Povolení vydávat příkazy za účelem správy prostředků produktu IBM MQ pouze autorizovaným administrátorem.
- Povolení k připojení aplikace ke správci front pouze tehdy, je-li k tomu přidružené ID uživatele přidružené k aplikaci.
- Povolení, aby aplikace otevřela pouze ty fronty, které jsou nezbytné pro jeho funkci.
- Povolení odběru aplikace pouze pro ta témata, která jsou nezbytná pro jeho funkci.
- Povolení, aby aplikace prováděla pouze operace ve frontě, které jsou nezbytné pro její funkci. Aplikace může například vyžadovat pouze procházení zpráv v určité frontě a nevložení nebo získání zpráv.

Další informace o tom, jak nastavit autorizaci, najdete v tématu “Plánování autorizace” na stránce 83 a přidružených dílčích tématech.

Související pojmy

“Autorizace” na stránce 6

Autorizace chrání kritické prostředky v systému omezením přístupu pouze k autorizovaným uživatelům a jejich aplikacím. Brání neautorizovanému použití prostředku nebo použití prostředku neoprávněným způsobem.

Auditování v IBM MQ

IBM MQ může vydávat zprávy událostí k záznamu, že došlo k neobvyklé aktivitě.

Zde je několik příkladů auditování v prostředí produktu IBM MQ :

- Aplikace se pokouší otevřít frontu, která není autorizována k otevření. Je vydána zpráva o události přípravy nástrojů. Prozkoumáním zprávy události zjistíte, že k tomuto pokusu došlo a může rozhodnout, jaká akce je nezbytná.
- Aplikace se pokusí otevřít kanál, ale pokus selže, protože zabezpečení SSL neumožňuje připojení. Je vydána zpráva o události přípravy nástrojů. Prozkoumáním zprávy události zjistíte, že k tomuto pokusu došlo a může rozhodnout, jaká akce je nezbytná.

Související pojmy

“Auditování” na stránce 6

Auditování je proces zaznamenávání a kontroly událostí za účelem zjištění, zda došlo k neočekávané nebo neautorizované aktivitě, nebo zda byl proveden pokus o provedení takové aktivity.

Důvěrnost v IBM MQ

Důvěryhodnost v produktu IBM MQ můžete implementovat zašifrováním zpráv.

Utajení může být zajištěno v prostředí produktu IBM MQ takto:

- Jakmile odesílající agent MCA obdrží zprávu z přenosové fronty, produkt IBM MQ pomocí protokolu TLS zašifruje zprávu před tím, než je odeslána prostřednictvím sítě do přijímajícího agenta MCA. Na druhém konci kanálu je zpráva dešifrována před tím, než ji agent MCA ukládá do cílové fronty.
- Zatímco zprávy jsou uloženy v lokální frontě, mohou být mechanizmy řízení přístupu poskytované produktem IBM MQ považovány za dostatečné pro ochranu jejich obsahu před neoprávněným zveřejněním. Avšak pro vyšší úroveň zabezpečení můžete použít produkt Advanced Message Security k šifrování zpráv uložených ve frontách.
- z/OS V 9.2.0 Zprávy uložené v lokálních frontách mohou být šifrovány v klidu s použitím šifrování datové sady produktu z/OS .

  Informace naleznete v části Důvěrnost dat v produktu IBM MQ for z/OS s šifrováním datové sady. Další informace viz.

Související pojmy

“Důvěrnost” na stránce 7

Služba *confidentiality* chrání citlivé informace před neoprávněným zveřejněním.

Integrita dat v produktu IBM MQ

Službu integrity dat můžete použít ke zjištění, zda byla zpráva upravena.

Integritu dat lze zajistit v prostředí produktu IBM MQ následujícím způsobem:

- TLS můžete použít ke zjištění toho, zda byl obsah zprávy během přenosu po síti úmyslně změněn. V TLS poskytuje algoritmus kódu digest zprávy detekce upravených zpráv při přenosu.

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

  Produkt IBM MQ při příjmu zpráv zjišťuje změněné zprávy; při příjmu upravené zprávy příkaz IBM MQ vyvolá chybovou zprávu AMQ9661 a kanál se zastaví.
- Zatímco zprávy jsou uloženy v lokální frontě, mohou být mechanizmy řízení přístupu poskytované produktem IBM MQ považovány za dostatečné pro zabránění záměrné úpravě obsahu zpráv.

Avšak pro vyšší úroveň zabezpečení můžete pomocí produktu Advanced Message Security zjistit, zda obsah zprávy byl mezi časem vložení zprávy do fronty a času načtenou z fronty úmyslně změněn.

Po zjištění upravené zprávy se aplikace pokoušející se o přijetí zprávy přijme návratový kód 2063 a v případě použití volání MQGET je zpráva přesunuta do SYSTEM.PROTECTION.ERROR.QUEUE

Související pojmy

"Integrita dat" na stránce 7
Služba *integrita dat* zjišťuje, zda došlo k neautorizované úpravě dat.

Šifrování v produktu IBM MQ

Produkt IBM MQ poskytuje šifrování pomocí protokolu TLS (Transport Security Layer).

Další informace viz "Protokoly zabezpečení TLS v produktu IBM MQ" na stránce 22.

Související pojmy

"Koncepce šifrování" na stránce 7
Tato kolekce témat popisuje koncepty šifrování použitelné pro produkt IBM MQ.

Protokoly zabezpečení TLS v produktu IBM MQ

Produkt IBM MQ podporuje protokol TLS (Transport Layer Security) k poskytování zabezpečení na úrovni odkazů pro kanály zpráv a kanály MQI.

Kanály zpráv a kanály MQI mohou používat protokol TLS k zajištění zabezpečení na úrovni odkazů. Volající MCA je klient TLS a agent MCA odezvy je serverem TLS.

V 9.2.0 Produkt IBM MQ podporuje verze 1.2 a 1.3 protokolu TLS. Starší verze TLS, stejně jako SSL, nejsou ve výchozím nastavení povoleny, ale mohou být v případě potřeby. Šifrovací algoritmy používané protokolem TLS můžete určit zadáním hodnoty CipherSpec jako součásti definice kanálu.

V 9.2.0 Seznam CipherSpecs podporovaných produktem IBM MQ a "Zamítnuté specifikace CipherSpecs" na stránce 424 pro ty, které jsou zamítnuty, naleznete v tématu "Povolení CipherSpecs" na stránce 408 .

Parametry SECPROT a SSLCIPH můžete použít k zobrazení protokolu zabezpečení a CipherSpec v kanálu.

Na každém konci kanálu zpráv a na konci serveru kanálu MQI pracuje agent MCA v zastoupení správce front, k němuž je připojen. Během komunikace výměnou potvrzení TLS odesílá agent MCA digitální certifikát správce front svému partnerskému agentu MCA na druhém konci kanálu. Kód IBM MQ na straně klienta kanálu MQI jedná jménem uživatele klientské aplikace IBM MQ . Při navázání komunikace TLS odesílá kód produktu IBM MQ digitální certifikát uživatele do agenta MCA na konci kanálu kanálu MQI.

Správci front a klienti klienta IBM MQ nemusí mít k sobě přidruženy osobní digitální certifikáty, pokud se chovají jako klienti TLS, pokud není na straně serveru kanálu uvedeno SSLCAUTH (POŽADOVÁNO).

Digitální certifikáty jsou uloženy v *úložišti klíčů*. Atribut správce front **SSLKeyRepository** určuje umístění úložiště klíčů, ve kterém je uložen digitální certifikát správce front. V systému klienta IBM MQ určuje proměnná prostředí MQSSLKEYR umístění úložiště klíčů, které zadržuje digitální certifikát uživatele. Alternativně může klientská aplikace IBM MQ zadat své umístění v poli **KeyRepository** ve struktuře voleb konfigurace TLS, MQSCO, na volání MQCONNX. Další informace o klíčových úložištích a o tom, jak určit, kde jsou umístěny, najdete v souvisejících tématech.

Podpora pro TLS

V 9.2.0 Produkt IBM MQ poskytuje podporu pro TLS 1.2 a TLS 1.3 na všech platformách. Další informace o protokolu TLS najdete 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 integrální součástí operačního systému IBM i .

z/OS
Podpora TLS je integrální součástí operačního systému z/OS . Podpora TLS v systému z/OS je známá jako *System SSL*.

Informace o nezbytných předpokladech pro podporu zabezpečení IBM MQ TLS viz Systémové požadavky pro IBM MQ.

Související pojmy

“Kryptografické bezpečnostní protokoly: TLS” na stránce 14
Kryptografické protokoly zajišťují zabezpečená spojení, což umožňuje dvěma stranám komunikovat s ochranou soukromí a integrity dat. Protokol Transport Layer Security (TLS) se vyvinul z zabezpečení SSL (Secure Sockets Layer). IBM MQ podporuje 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 využívají obecný termín *úložiště klíčů* k popisování úložiště pro digitální certifikáty a jejich přidružené soukromé klíče. Na úložiště klíčů se odkazují různé názvy na různých platformách a prostředí, které 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: *key database file*
- z/OS V systému z/OS: *keyring*

Další informace naleznete v tématech “digitální certifikáty” na stránce 9 a “Koncepce zabezpečení přenosové vrstvy (TLS)” na stránce 14.

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

- Řada 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 IBM MQ MQI clientpřidružíte samostatný osobní certifikát. Osobní certifikáty jsou nezbytné pro klienta TLS, je-li požadováno vzájemné ověření. Není-li vyžadováno vzájemné ověření, osobní certifikáty nejsou na straně klienta potřeba. Úložiště klíčů může také obsahovat soukromý klíč odpovídající každému osobnímu certifikátu.
- Žádosti o certifikát, které čekají na podpis pomocí důvěryhodného certifikátu CA.

Další informace o ochraně úložiště klíčů naleznete v tématu “Ochrana úložišť klíčů IBM MQ” na stránce 24.

Umístění úložiště klíčů závisí na platformě, kterou používáte:

IBM i **IBM i**

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

Případně můžete zadat, že má být místo toho použito systémové úložiště certifikátů systému IBM i . Chcete-li tuto změnu provést, změňte hodnotu atributu **SSLKEYR** správce front na *SYSTEM. Tato

hodnota označuje, že správce front musí používat úložiště certifikátů systému a správce front je registrován pro použití jako aplikace s produktem Digital Certificate Manager (DCM).

Paměť certifikátů také obsahuje soukromý klíč pro správce front.

ALW **Systémy AIX, Linux, and Windows**

Klíčovým databázovým souborem je úložiště klíčů. Název souboru databáze klíčů musí mít příponu `.kdb`. Například v systému AIX and Linuxje výchozí soubor databáze klíčů pro správce front `QM1` `/var/mqm/qmgrs/QM1/ssl/key.kdb`. Je-li produkt IBM MQ nainstalován ve výchozím umístění, ekvivalentní cesta na serveru Windows je `C:\ProgramData\IBM\MQ\Qmgrs\QM1\ssl\key.kdb`.

Každý soubor databáze klíčů má přidružený soubor pro uložení hesla. Tento soubor obsahuje kódovaná hesla, která umožňují programům přístup k databázi klíčů. Soubor pro uložení hesla musí být ve stejném adresáři a musí mít stejný soubor 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. Jsou-li certifikáty a klíče uchovávány na kartách PKCS #11 , IBM MQ stále vyžaduje přístup k souboru databáze klíčů a k souboru pro uložení hesla.

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 **z/OS**

Certifikáty se nacházejí ve svazku klíčů v produktu z/OS.

Ostatní externí správci zabezpečení (ESM) také používají svazek 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 má přístup k souboru úložiště klíčů pouze zamýšlený uživatel. Tím zabráníte tomu, aby narušitel nebo jiný neautorizovaný uživatel kopíroval soubor úložiště klíčů do jiného systému, a poté v systému, který má zosobňovat požadovaného uživatele, nastavení identického ID uživatele.

Oprávnění na souborech závisí na uživatelské umask a který nástroj se používá. V systému Windowsvyžadují účty IBM MQ oprávnění `BypassTraverseChecking` , což znamená, že oprávnění složek v cestě k souboru nemají žádný vliv.

Zkontrolujte oprávnění k souborům v souborech úložiště klíčů a ujistěte se, že soubory a obsahující složku nejsou čitelnější na světě, pokud možno ani nečitelné pro skupinu.

Nastavení úložiště klíčů jen pro čtení je dobrým zvykem, na libovolném systému, který používáte, přičemž pouze administrátor může povolit operace zápisu, aby bylo možné provést údržbu.

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

Digitální certifikáty certifikátu, základní informace o požadavcích

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

Co je jmenovka certifikátu?

Označení certifikátu je jedinečný identifikátor představující digitální certifikát uložený v úložišti klíčů a poskytuje vhodný čitelný název, se kterým se bude odkazovat na konkrétní certifikát při provádění funkcí správy klíčů. Návěští certifikátu přiřazujete při prvním přidání certifikátu k úložišti klíčů.

Návěští 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 rámci certifikátu samotného. Ty jsou definovány při vytvoření certifikátu a nelze je změnit. Je-li to nezbytné, můžete změnit popisek přidružený k digitálnímu certifikátu.

Syntaxe návěští certifikátu

Označení certifikátu může obsahovat písmena, čísla a interpunkční znaky za následujících podmínek:

- Multi Návěští certifikátu může obsahovat až 64 znaků.
- z/OS Návěští certifikátu může obsahovat až 32 znaků.
- Označení certifikátu může obsahovat mezery.
- Štítky rozlišují velikost písmen.
- V systémech, které používají EBCDIC katakana, nemůžete používat malá písmena.

Další požadavky na hodnoty označení certifikátu jsou uvedeny v následujících sekcích.

Jak se používá jmenovka certifikátu?

IBM MQ používá návěští certifikátu k nalezení osobního certifikátu, který se odešle během navázání komunikace TLS. Tím vyloučíte nejednoznačnost, pokud v úložišti klíčů existuje více než jeden osobní certifikát.

Označení certifikátu můžete nastavit na hodnotu dle vlastního výběru. Pokud nenastavíte žádnou hodnotu, použije se výchozí popisek podle konvence pojmenování v závislosti na použité platformě. Podrobnosti viz sekce, které následují, o konkrétních platformách.

Notes:

1. Označení certifikátu nelze nastavit na systémech Java nebo JMS .
2. Automaticky definované kanály vytvořené uživatelskou procedurou automatické definice kanálu (CHAD) nemohou nastavit jmenovku certifikátu, protože k navázání komunikace TLS došlo v době vytvoření kanálu. Nastavení štítku certifikátu v uživatelské proceduře CHAD pro příchozí kanály nemá žádný účinek.

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

Během komunikace výměnou potvrzení TLS vždy klient TLS získává a ověřuje digitální certifikát ze serveru. Při použití implementace produktu IBM MQ server TLS vždy požaduje certifikát od klienta a klient vždy poskytuje certifikát serveru, pokud je nalezen. Pokud klient nemůže najít osobní certifikát, pošle klientovi odpověď no `certificate` na server.

Server TLS vždy ověřuje platnost certifikátu klienta, je-li odeslán. Pokud klient neodešle certifikát, ověření selže, pokud je konec kanálu, který se chová jako server TLS, definován buď s parametrem **SSLCAUTH** nastaveným na hodnotu *POVINNÍ* nebo nastaveným na hodnotu parametru **SSLPEER** .

Všimněte si, že příchozí kanály (včetně příjemce, žadatele, příjemce klastru, nekvalifikovaný server a kanály připojení serveru) odešlou pouze konfigurovaný certifikát pouze v případě, že verze produktu IBM MQ vzdáleného peeru plně podporuje konfiguraci popisku certifikátu a kanál používá TLS CipherSpec.

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

Ve všech ostatních případech parametr **CERTLABL** správce front určuje odeslaný certifikát. Zejména následující vždy obdrží certifikát nakonfigurovaný parametrem **CERTLABL** správce front, bez ohledu na nastavení jmenovky specifické pro daný kanál:

- Klienti Java a JMS podporují indikaci SNI (Server Name Indication), tj. certifikáty na kanálu podle jednotlivých kanálů.
- Verze produktu IBM MQ před verzí IBM MQ 8.0.
- Spravované klienty .NET

Kromě toho musí být certifikát použitý pro kanál vhodný pro kanál CipherSpec -další informace naleznete v dokumentu “Digitální certifikáty a kompatibilita CipherSpec v produktu IBM MQ” na stránce 43 .

Produkt IBM MQ 8.0 a novější podporuje použití více certifikátů ve stejném správci front s použitím štítku certifikátu na kanál zadaný pomocí atributu **CERTLABL** v definici kanálu. Příchozí kanály správci front

(například připojení k serveru nebo příjemce) se spoléhají na zjištění názvu kanálu pomocí protokolu SNI (TLS Server Name Indication), aby mohl předložit správný certifikát od správce front. Další informace o použití více certifikátů ve správci front naleznete v tématu “Jak produkt IBM MQ poskytuje schopnost více certifikátů” na stránce 27.

Pokud se kanál připojuje k cílovému správci front prostřednictvím produktu IBM MQ Internet Pass-Thru (MQIPT) a přenosová cesta MQIPT má nastaveny jak **SSLServer** , tak **SSLClient** , existují dvě samostatné relace TLS mezi koncovými body. Ve verzích starších než IBM MQ 9.2.5se data SNI neprojdou přes přerušení relace. Zabráníte tak použití certifikátu na kanál v cílovém správci front pro připojení

TLS mezi produktem MQIPT a správcem front. V 9.2.5 Z produktu IBM MQ 9.2.5lze nakonfigurovat produkt MQIPT tak, aby povoloval správce cílových front více certifikátů, a to buď nastavením rozhraní SNI na název kanálu, nebo předáním prostřednictvím rozhraní SNI přijaté v rámci příchozího připojení k přenosové cestě. Další informace o podpoře více certifikátů a produktu MQIPTnaleznete v tématu IBM MQ s podporou více certifikátů pomocí produktu MQIPT.

Další informace o připojení správce front s použitím jednosměrného ověření, tj. když klient TLS neodešle certifikát, najdete v tématu Připojení dvou správců front s použitím jednosměrného ověření.

Multiformní systémy

Multi

V systému Multiplatformsodešle server TLS certifikát klientovi.

Pro správce front a klienty jsou následující zdroje prohledávány v posloupnosti pro neprázdnou hodnotu. První neprázdná hodnota určuje jmenovku certifikátu. Označení certifikátu musí existovat v úložišti klíčů. Pokud není nalezen odpovídající certifikát ve správném případě a formátu, který odpovídá štítku, dojde k chybě a navázání komunikace TLS se nezdaří.

Správci front

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

IBM MQ klienti

1. Atribut popisku certifikátu **CERTLABL** v definici kanálu CLNTCONN.
2. Struktura struktury MQSCO **`CertificateLabel`** .
3. Proměnná prostředí **MQCERTLABL**.
4. Client `.ini` file (in its SSL section) **`CertificateLabel`** attribute
5. Předvolba, která je ve formátu: `ibmwebspheremq` s ID uživatele, ke kterému je aplikace klienta spuštěna jako připojená, a to vše malými písmeny. Například pro ID uživatele produktu USER1je výchozí popisek certifikátu `ibmwebspheremquser1`.

z/OS systémy

z/OS

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

Pro správce front a klienty jsou následující zdroje prohledávány v posloupnosti pro neprázdnou hodnotu. První neprázdná hodnota určuje jmenovku certifikátu. Označení certifikátu musí existovat v úložišti klíčů. Pokud není nalezen odpovídající certifikát ve správném případě a formátu, který odpovídá štítku, dojde k chybě a navázání komunikace TLS se nezdaří.

1. Atribut štítku certifikátu kanálu, **CERTLABL**.
2. Je-li sdílený, atribut návěští certifikátu skupiny sdílení front **CERTQSGL**.

   Pokud není sdílený, atribut návěští certifikátu správce front **CERTLABL**.
3. Výchozí hodnota, která je 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 zobrazen. Například pro správce front s názvem `QM1`je výchozí jmenovka certifikátu `ibmWebSphereMQQM1`.
4. Pokud není nalezen certifikát s formátem ve volbě “3” na stránce 27, IBM MQ se pokusí použít certifikát označený jako výchozí v souboru svazku klíčů.

Informace o tom, jak zobrazit úložiště klíčů, viz “Vyhledání úložiště klíčů pro správce front v systému z/OS” na stránce 312.

Klienti IBM MQ Java a IBM MQ JMS

Klienti IBM MQ Java a IBM MQ JMS používají zařízení svého poskytovatele JSSE (Java Secure Socket Extension) k výběru osobního certifikátu během komunikace výměnou potvrzení TLS, a proto nejsou předmětem požadavků na návěští certifikátu.

Výchozí chování je, že klient JSSE iteruje certifikáty v úložišti klíčů výběrem prvního přijatelného osobního certifikátu, který byl nalezen. Toto chování je však pouze výchozí a je závislé na implementaci poskytovatele JSSE.

Kromě toho je rozhraní JSSE vysoce přizpůsobitelné konfigurací a přímým přístupem v době běhu aplikace. Konkrétní podrobnosti naleznete v dokumentaci dodané s poskytovatelem JSSE.

Při odstraňování problémů nebo lépe porozumět navázání komunikace prováděné klientskou aplikací produktu IBM MQ Java v kombinaci s konkrétním poskytovatelem JSSE můžete povolit ladění nastavením `javax.net.debug=ssl` v prostředí JVM.

Proměnnou můžete nastavit v aplikaci pomocí konfigurace nebo zadáním příkazu `-Djavax.net.debug=ssl` na příkazový řádek.

Linux *Jak produkt IBM MQ poskytuje schopnost více certifikátů*

Indikace SNI (Server Name Indication) je rozšířením protokolu TLS, který umožňuje klientovi označit, jaká služba to vyžaduje. V terminologii produktu IBM MQ se jedná o přirovnání ke kanálu.

Rozšíření SNI je používáno produktem IBM MQ k povolení více certifikátů, které mají být uvedeny v různých kanálech, pomocí parametru CERTLABL v definici kanálu.

Adresa SNI použitá produktem IBM MQ je založena na názvu kanálu, který je požadován, následován příponou `.chl.mq.ibm.com`.

Názvy kanálů produktu IBM MQ jsou mapovány na platné názvy SNI takto:

- Velká písmena A až Z jsou zalomena na malá písmena
- Číslice `0` až 9 jsou nezměněny.
- Všechny ostatní znaky, včetně malých písmen a až z, jsou převedeny na dvouciferný hexadecimální znakový kód ASCII (v případě malých písmen), za nímž následuje pomlčka.
  - Malá písmena velká a malá písmena a až z se mapují na hexadecimální `61-` na `7a-`
  - procento (%) mapuje na hexadecimální `25-`
  - pomlčka (-) mapuje na hexadecimální `2d-`
  - tečka (`.`) je mapována na hexadecimální `2e-`
  - dopředné lomítko (/) mapuje na hexadecimální `2f-`
  - podtržítko (_) mapuje na hexadecimální `5f-`

Na platformách EBCDIC se název kanálu převede na ASCII, než se toto mapování použije.

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

Naproti tomu nižší název kanálu případu `to.qmgr1` mapuje na adresu SNI produktu `74-6f-2e-71-6d-67-72-1.chl.mq.ibm.com`.

Poznámka: V prostředích, ve kterých musí být generovaná adresa URL SNI v souladu se specifikacemi formátování adresy URL, například když se klient připojuje ke správci front běžícím v produktu Red Hat® OpenShift® přes trasu Red Hat OpenShift , nesmí název kanálu končit malým písmenem.

Další vlastnost **OutboundSNI** sekce SSL vám umožňuje vybrat, zda se má SNI při inicializaci připojení TLS nastavit na název cílového kanálu IBM MQ pro vzdálený systém, nebo na název hostitele. Další informace o vlastnosti **OutboundSNI** naleznete v tématech Sekce SSL souboru qm.ini a Sekce SSL konfiguračního souboru klienta.

Více certifikátů vyžaduje, aby byl SNI nastaven na název kanálu IBM MQ . Je-li pro připojení ke kanálu produktu IBM MQ s nakonfigurovaným popiskem certifikátu použit název hostitele, vlastní nebo žádný adaptér SNI, bude připojená aplikace odmítnuta s chybou MQRC_SSL_INITIALIZATION_ERROR a v protokolech chyb vzdáleného správce front bude vytištěna zpráva AMQ9673 .

V 9.2.5 Pokud se kanál připojuje k cílovému správci front prostřednictvím produktu IBM MQ Internet Pass-Thru (MQIPT), musí být produkt MQIPT nakonfigurován tak, aby nastavil rozhraní SNI na název kanálu, nebo aby prošel prostřednictvím rozhraní SNI přijatého v příchozím připojení k přenosové cestě, aby bylo možné použít více certifikátů, které má správce cílové fronty používat. Další informace o podpoře více certifikátů a produktu MQIPTnaleznete v tématu IBM MQ s podporou více certifikátů pomocí produktu 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, správce front ihned nevybere nový obsah. Má-li správce front používat nový obsah úložiště klíčů, je třeba zadat příkaz REFRESH SECURITY TYPE (SSL).

Tento proces je záměrný a předchází situaci, kdy více spuštěných kanálů může používat různé verze úložiště klíčů. Jako ovládací prvek zabezpečení může správce front kdykoli načíst pouze jednu verzi úložiště klíčů.

Další informace o příkazu REFRESH SECURITY TYPE (SSL) naleznete v tématu REFRESH SECURITY.

Úložiště klíčů můžete také aktualizovat pomocí příkazů PCF nebo pomocí IBM MQ Explorer. Další informace naleznete v tématu Příkaz MQCMD_REFRESH_SECURITY a v tématu *Aktualizace zabezpečení TLS* v části IBM MQ Explorer této dokumentace k produktu.

Související pojmy
“Aktualizace pohledu klienta s obsahem úložiště klíčů SSL/TLS a nastavení SSl/TLS” na stránce 28
Chcete-li aktualizovat klientskou aplikaci s aktualizovaným obsahem úložiště klíčů, musíte aplikaci klienta zastavit a restartovat.

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

Na klientovi IBM MQ nelze obnovit zabezpečení; pro klienty neexistuje ekvivalent příkazu REFRESH SECURITY TYPE (SSL) (viz REFRESH SECURITY). pro další informace.

Chcete-li aktualizovat aplikaci klienta s aktualizovaným obsahem úložiště klíčů, musíte aplikaci ukončit a znovu spustit, kdykoli změníte certifikát zabezpečení.

Při restartování kanálu se obnoví konfigurace a v případě, že aplikace obsahuje logiku opětovného připojení, je možné zabezpečení aktualizovat na straně klienta zadáním příkazu STOP CHL STATUS (INACTIVE).

Související pojmy
“Aktualizace úložiště klíčů správce front” na stránce 28

Změníte-li obsah úložiště klíčů, správce front ihned nevybere nový obsah. Má-li správce front používat nový obsah úložiště klíčů, je třeba zadat příkaz REFRESH SECURITY TYPE (SSL).

Ochrana heslem MQCSP

V produktu IBM MQ 8.0můžete odesílat hesla, která jsou zahrnuta do struktury MQCSP, buď chráněna, pomocí funkčnosti produktu IBM MQ , nebo šifrováním pomocí šifrování TLS.

Důležité: Ochrana heslem MQCSP je užitečná pro účely testování a vývoje, protože použití ochrany heslem MQCSP je jednodušší než nastavení šifrování TLS, ale nikoli jako zabezpečené. Pro provozní účely byste měli používat šifrování TLS v preferencích k ochraně heslem produktu IBM MQ , zvláště je-li síť mezi klientem a správcem front nedůvěryhodná, protože šifrování TLS je bezpečnější.

Pokud se týká přesně toho, jaké šifrování se používá, a jakou ochranu nabízí, je třeba použít plné šifrování TLS. V této situaci jsou algoritmy veřejně známy a pro daný podnik můžete vybrat příslušný algoritmus pomocí atributu kanálu produktu **SSLCIPH** .

Další informace o struktuře MQCSP naleznete v tématu Struktura MQCSP.

Ochrana heslem se používá, jsou-li splněny všechny následující podmínky:

- Oba konce připojení používají produkt IBM MQ 8.0nebo novější.
- Kanál nepoužívá šifrování TLS. Kanál nepoužívá šifrování TLS, pokud má kanál prázdný atribut **SSLCIPH** , nebo je atribut **SSLCIPH** nastaven na hodnotu CipherSpec , která šifrování neposkytuje. Šifry NULL, například NULL_SHA, nezajišťují šifrování.
- Nastavili jste **MQCSP**.**AuthenticationType** pro MQCSP_AUTH_USER_ID_AND_PWD. Nastavení této hodnoty umožní vyhodnocení dalších kontrol při rozhodování o tom, zda je ochrana pomocí hesla provedena. Výchozí hodnota je **MQCSP**.**AuthenticationType** je MQCSP_AUTH_NONE. Při výchozím nastavení není ochrana heslem provedena. Další informace viz **AuthenticationType**.
- Pokud je klient IBM MQ Explorer a režim kompatibility identifikace uživatele není povolen, což není výchozí nastavení. Tato podmínka je použitelná pouze pro Průzkumníka IBM MQ .

Pokud tyto podmínky nejsou splněny, heslo se odešle jako prostý text, pokud není zakázáno nastavením konfigurace produktu **PasswordProtection** .

Nastavení konfigurace produktu PasswordProtection

Atribut **PasswordProtection** v sekci Channels v konfiguračním souboru klienta a souboru INI správce front může zabránit odesílání hesel v prostém textu. Atribut může mít jednu z následujících hodnot. Předvolená hodnota je `compatible`:

Kompatibilní

Heslo lze odesílat jako prostý text, je-li správce front nebo klient spuštěn ve verzi produktu IBM MQ starší než IBM MQ 8.0. To znamená, že hesla v prostém textu jsou povolena pro kompatibilitu.

Proto:

- Heslo je odesláno zašifrováno pomocí TLS CipherSpec , je-li použito šifrování TLS a CipherSpec nemá hodnotu null.
- Heslo je odesláno jako prostý text, pokud správce front nebo klient spouští verzi produktu IBM MQ starší než IBM MQ 8.0a šifrování TLS se nepoužívá. Heslo se odešle jako prostý text, protože verze produktu IBM MQ starší než IBM MQ 8.0 mohou odesílat hesla pouze v prostém textu.
- Heslo je chráněno, pokud správce front i klient spouští verzi produktu IBM MQ na adrese IBM MQ 8.0 nebo novější a používá se buď hodnota CipherSpec s hodnotou null, nebo šifrování TLS není použito. **MQCSP**Hodnota **AuthenticationType** musí být nastavena na hodnotu MQCSP_AUTH_USER_ID_AND_PWD.
- Dojde k selhání připojení před odesláním hesla, pokud správce front i klient spouští verzi produktu IBM MQ na IBM MQ 8.0 nebo pozdější a **MQCSP**.**AuthenticationType** není nastaveno na MQCSP_AUTH_USER_ID_AND_PWD.

Vždy
Heslo musí být buď zašifrováno se CipherSpec , která není null CipherSpec, nebo **MQCSP**.Hodnota **AuthenticationType** musí být nastavena na hodnotu MQCSP_AUTH_USER_ID_AND_PWD. Jinak se připojení nezdaří. To znamená, že hesla v prostém textu nejsou povolena.

Proto:

- Heslo je odesláno zašifrováno pomocí TLS CipherSpec , je-li použito šifrování TLS a CipherSpec nemá hodnotu null.
- Heslo je chráněno, pokud správce front i klient spouští verzi produktu IBM MQ na serveru IBM MQ 8.0 nebo později, a nepoužívá se šifrování TLS, nebo je použita hodnota CipherSpec s hodnotou null. **MQCSP**Hodnota **AuthenticationType** musí být nastavena na hodnotu MQCSP_AUTH_USER_ID_AND_PWD.
- Připojení selže před odesláním hesla, pokud správce front nebo klient spouští verzi produktu IBM MQ starší než verze IBM MQ 8.0a šifrování TLS se nepoužívá. Vzhledem k tomu, že verze produktu IBM MQ starší než IBM MQ 8.0 mohou odesílat hesla pouze v prostém textu a produkt `always` vyžaduje, aby bylo heslo buď šifrováno, nebo chráněno, připojení selže.

volitelné
Heslo lze volitelně poslat jako chráněné, ale je odesláno jako prostý text, je-li **MQCSP**.**AuthenticationType** není nastaveno na MQCSP_AUTH_USER_ID_AND_PWD. To znamená, že hesla v prostém textu mohou být odesílána libovolným klientem.

Proto:

- Heslo je odesláno zašifrováno pomocí TLS CipherSpec , je-li použito šifrování TLS a CipherSpec nemá hodnotu null.
- Heslo je odesláno jako prostý text, je-li použita hodnota CipherSpec s hodnotou Null a **MQCSP**.**AuthenticationType** není nastaveno na MQCSP_AUTH_USER_ID_AND_PWD.
- Heslo je odesláno jako prostý text, pokud správce front nebo klient spouští verzi produktu IBM MQ starší než IBM MQ 8.0a šifrování TLS se nepoužívá. Heslo se odešle jako prostý text, protože verze produktu IBM MQ starší než IBM MQ 8.0 mohou odesílat hesla pouze v prostém textu.
- Heslo je chráněno, pokud správce front i klient spouští verzi produktu IBM MQ na adrese IBM MQ 8.0 nebo novější, šifrování TLS se nepoužívá, nebo je použito hodnoty CipherSpec s hodnotou null a **MQCSP**.**AuthenticationType** je nastaven na hodnotu MQCSP_AUTH_USER_ID_AND_PWD.

varování
Hesla prostého textu mohou být odesílána libovolným klientem. Je-li do protokolů chyb správce front přijato heslo v prostém textu, je do správce front zapsána varovná zpráva (AMQ9297).

U klientů Java a JMS se chování atributu **PasswordProtection** mění závislosti na volbě použití režimu kompatibility nebo režimu MQCSP:

- Pokud klienti Java a JMS pracují v režimu kompatibility, struktura MQCSP se během zpracování připojení netečí k toku. Proto je chování atributu **PasswordProtection** stejné chování, jaké je popsáno u klientů, kteří mají spuštěnou verzi produktu IBM MQ starší než IBM MQ 8.0.
- Pokud klienti Java a JMS pracují v režimu MQCSP, chování atributu **PasswordProtection** je chování podle popisu.

Další informace o ověření připojení s klienty Java a JMS viz "Ověření spojení s klientem Java" na stránce 76.

Správce digitálních certifikátů (DCM)

Použijte produkt DCM ke správě digitálních certifikátů a soukromých klíčů na 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 zpracovat digitální certifikáty od certifikačních autorit (CA) nebo jiných třetích stran. Pro vytvoření a správu digitálních certifikátů pro své uživatele můžete také sloužit jako lokální vydavatel certifikátů.

Produkt DCM také podporuje používání seznamů CRL (Certificate Revocation Lists) k poskytování silnějšího certifikátu a procesu ověření platnosti aplikací. Produkt DCM můžete použít k definování umístění, kde se na serveru LDAP nachází specifický vydavatel certifikátů CRL, takže produkt IBM MQ může ověřit, že specifický certifikát nebyl odvolán.

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

DCM poskytuje uživatelské rozhraní založené na browseru, které můžete použít ke správě digitálních certifikátů pro vaše aplikace a uživatele. Uživatelské rozhraní se dělí na dva hlavní rámce: navigační rámec a rámec úloh.

Navigační lišta se používá k výběru úloh pro správu certifikátů nebo aplikací, které je používají. Některé jednotlivé úlohy se zobrazují 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 asistované úlohy, jako např. Zobrazit certifikát, Obnovit certifikát a Importovat certifikát. Je-li položka v navigačním rámci kategorie, která obsahuje více než jednu úlohu, zobrazí se šipka vlevo od ní. Šipka označuje, že když vyberete odkaz na kategorii, zobrazí se rozbalený seznam úloh, které vám umožní vybrat si, která úloha se má provést.

Důležité informace o produktu DCM najdete v následujících publikacích IBM Redbooks :

- *IBM i Wired Network Security: OS/400 V5R1 DCM and Cryptographic Enhancements*, SG24-6168. Konkrétně se podívejte na dodatky pro základní informace o nastavení vašeho systému IBM i jako lokálního CA.
- *AS/400 Internet Security: Developing a Digital Certificate Infrastructure*, SG24-5659. Konkrétně viz kapitola 5. *Digital Certificate Manager for AS/400* , který vysvětluje DCM AS/400 .

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" . Certifikát pro tento modul byl přesunut do historického stavu. Zákazníci by si měli prohlédnout IBM Crypto for C certificate a měli by si být vědomi jakýchkoli 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 32.

z/OS Další informace o shodě FIPS 140-2 IBM MQ připojení TLS v systému z/OSviz “Federální standardy zpracování informací (FIPS) pro z/OS” na stránce 34.

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 264
Vytvořte úložiště klíčů pomocí softwaru vyhovujícího standardu FIPS a poté určete, že kanál musí používat specifikace CipherSpecss certifikací FIPS.

"Správa digitálních certifikátů pomocí produktů runmqckm, runmqakma strmqikm" na stránce 279
V systémech AIX, Linux, and Windows spravujte klíče a digitální certifikáty pomocí konzoly **strmqikm** (iKeyman). GUI, 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 19
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 na kanálu SSL/TLS v systémech AIX, Linux, and Windows vyžadováno šifrování, produkt IBM MQ používá 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" . Certifikát pro tento modul byl přesunut do historického stavu. Zákazníci by si měli prohlédnout IBM Crypto for C certificate a měli by si být vědomi jakýchkoli 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 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, jako např. **runmqakm** s volbou `-fips` .
- Pro všechny aplikace IBM MQ MQI client připojení používá sadu 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, jako např. **runmqakm** s volbou `-fips` .
- 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 má být použito 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, jako např. **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 má být použito 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, jako např. **runmqakm** s volbou `-fips` .
- Pro nespravované klientské aplikace .NET používá připojení sadu 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 .NET .
  - Všechna úložiště klíčů byla vytvořena a byla s nimi manipulována pouze pomocí softwaru vyhovujícího standardu FIPS, jako např. **runmqakm** s volbou `-fips` .
- Pro nespravované klientské aplikace XMS .NET používá připojení sadu 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 dokumentaci XMS .NET .
  - Všechna úložiště klíčů byla vytvořena a byla s nimi manipulována pouze pomocí softwaru vyhovujícího standardu FIPS, jako např. **runmqakm** s volbou `-fips` .

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 GSKit je 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 zjistit aktuálně nainstalovanou verzi ICC, spusťte příkaz **dspmqver -p 64 -v** .

Zde je příklad extraktu výstupu **dspmqver -p 64 -v** týkajícího se ICC:

```
ICC-mezinárodní
============
@ (#)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 produkt GSKit ICC 8 (obsažený v sadě GSKit 8) lze nalézt na následující adrese: Program pro ověření šifrovacího modulu.

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 nakonfigurován tak, aby pracoval v souladu se standardem FIPS 140-2, jsou ve vztahu k specifikacím Triple DES (3DES) CipherSpecsvynucena další omezení. 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 454.

Produkt IBM MQ generuje klíče relace Triple DES, které již splňují pravidla 1 a 2. Chcete-li však splnit třetí omezení, musíte při použití specifikací Triple DES CipherSpecs v konfiguraci FIPS 140-2 povolit reset tajného klíče. 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 264
Vytvořte úložiště klíčů pomocí softwaru vyhovujícího standardu FIPS a poté určete, že kanál musí používat specifikace CipherSpecss certifikací FIPS.

“Správa digitálních certifikátů pomocí produktů runmqckm, runmqakma strmqikm” na stránce 279
V systémech AIX, Linux, and Windows spravujte klíče a digitální certifikáty pomocí konzoly **strmqikm** (iKeyman). GUI, 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 19
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 *Federální standardy zpracování informací (FIPS) pro z/OS*

Je-li šifrování vyžadováno v kanálu SSL/TLS v produktu z/OS , používá produkt IBM MQ službu s názvem System SSL. Cílem System SSL je poskytovat funkce k bezpečnému spuštění v režimu, který je navržen pro dodržení standardu FIPS (Federal Information Processing Standards) of the US National Institute of Standards and Technology, na úrovni 140-2.

Při implementaci připojení vyhovujících standardu FIPS 140-2 s připojeními IBM MQ TLS existuje řada bodů, které je třeba vzít v úvahu:

- Chcete-li povolit kanály zpráv produktu IBM MQ pro prostředí FIPS-slučitelnost, ujistěte se, že jsou splněny následující podmínky:
  - Produkt System SSL Security Level 3 FMID je instalován a konfigurován (viz Plánování instalace produktu IBM MQ).

– Systémové moduly SSL jsou ověřovány.
– Atribut SSLFIPS správce front byl nastaven na hodnotu **YES**.

Při provádění v režimu FIPS využívá System SSL při práci obslužný program CP Assist for Cryptographic Function (CPACF). Kryptografické funkce podporované hardwarem ICSF, pokud jsou spuštěny v režimu non-FIPS, jsou i nadále využívány při provádění v režimu FIPS, s výjimkou generování podpisu RSA, který musí být proveden v softwaru.

Tabulka 2. Rozdíly mezi režimem režimu FIPS a podporou algoritmu non-FIPS.

	Ne-FIPS		**FIPS**	
algoritmus	**Velikosti klíče**	**Hardware**	**Velikosti klíče**	**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
DSA	512-1024		1024	
DH	512-2048		2048	

V režimu FIPS System SSL může používat pouze certifikáty, které používají algoritmy a velikosti klíčů uvedené v tabulce 1. Během ověřování certifikátu X.509 , je-li zjištěn algoritmus, který je nekompatibilní s režimem FIPS, nelze certifikát použít a je považován za neplatný.

Pro aplikace tříd produktu IBM MQ používající režim klienta v rámci produktu WebSphere Application Server se podívejte na Podpora standardu FIPS (Federal Information Processing Standard).

Informace o konfiguraci System SSL naleznete v tématu Nastavení ověření modulu systémového zabezpečení SSL.

Související odkazy

“Federální standardy zpracování informací” na stránce 19
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 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 v atributech **CERTLABL** uveden popisek certifikátu. Při vytváření kanálu jste udělali chybu v atributu **CERTLABL** kanálu, takže když se klient pokusí o připojení, 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 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 sady 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 zabezpečení TLS na klientech. Použití TLS můžete upravit různými způsoby.

Produkt IBM MQ poskytuje podporu TLS pro produkt IBM MQ MQI clients v systémech AIX, Linux, and Windows . Používáte-li produkt IBM MQ classes for Java, přečtěte si téma Použití produktu IBM MQ classes for Java a pokud používáte produkt IBM MQ classes for JMS, viz téma Použití produktu IBM MQ classes for JMS. Zbývající část tohoto oddílu se nevztahuje na prostředí Java nebo JMS .

Úložiště klíčů pro IBM MQ MQI client můžete určit buď pomocí hodnoty MQSSLKEYR v konfiguračním souboru klienta IBM MQ , nebo při volání aplikace MQCONNX. K určení, že kanál používá TLS, máte tři možnosti:

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

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

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

Pokud jsou na klientském počítači provedeny změny obsahu úložiště klíčů TLS, umístění úložiště klíčů TLS, informací o ověření nebo šifrovacích parametrů hardwaru, je třeba 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. Všechny nové nastavení TLS se použijí. Tato nastavení jsou analogická k těm nastavením obnovených příkazem REFRESH SECURITY TYPE (SSL) v systémech správce front.

Je-li produkt IBM MQ MQI client spuštěn v systému AIX, Linux, and Windows s kryptografickým hardwarem, nakonfigurujte tento hardware s proměnnou prostředí MQSSLCRYP. Tato proměnná je ekvivalentní parametru SSLCRYP v příkazu ALTER QMGR MQSC. Popis parametru SSLCRYP v příkazu ALTER QMGR MQSC najdete v tématu ALTER QMGR (popis parametru SSLCRYP). Pokud použijete verzi parametru SSLCRYP GSK_PCS11 , musí být popisek tokenu PKCS #11 určen zcela v menším případě.

Resetování tajných klíčů TLS a FIPS jsou podporovány na IBM MQ MQI clients. Další informace naleznete v tématech “Resetování tajných klíčů SSL a TLS” na stránce 454 a “Standard FIPS (Federal Information Processing Standards) pro AIX, Linux, and Windows” na stránce 32.

Další informace o podpoře TLS pro produkt IBM MQ MQI clientsviz “Nastavení zabezpečení produktu IBM MQ MQI client” na stránce 263 .

Související úlohy

Konfigurace klienta pomocí konfiguračního souboru

Určení, že kanál MQI používá SSL/TLS

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

Pro tento atribut můžete následujícím způsobem definovat kanál připojení klienta s hodnotou tohoto atributu. Jsou uvedeny v pořadí s klesající prioritou.

1. Když uživatelská procedura PreConnect poskytuje strukturu definice kanálu, která má být použita.

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

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

   Aplikace může určit název CipherSpec v poli *SSLCipherSpec* struktury definice kanálu, MQCD.Na tuto strukturu se odkazuje struktura voleb připojení, MQCNO, což je parametr 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 použít parametr SSLCIPH v příkazu k určení názvu CipherSpec.

4. Použití Active Directory na systému Windows.

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

Pokud například klientská aplikace poskytuje definici kanálu připojení klienta ve struktuře MQCD v rámci volání MQCONNX, tato definice se používá přednostně k položkám v tabulce definic kanálů klienta, ke které může klient produktu IBM MQ přistupovat.

K poskytnutí definice kanálu na straně klienta kanálu MQI, který používá TLS, nelze použít proměnnou prostředí MQSERVER.

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

Související pojmy

"Určení CipherSpec pro IBM MQ MQI client" na stránce 432

Pro specifikaci CipherSpec pro produkt IBM MQ MQI clientjsou k dispozici tři možnosti.

CipherSpecs a CipherSuites v produktu IBM MQ

Produkt IBM MQ podporuje algoritmy TLS1.3 a TLS 1.2 CipherSpecsa RSA a Diffie-Hellman. Můžete však povolit zamítnutý CipherSpecs, pokud to potřebujete.

Informace o následujících tématech viz "Povolení CipherSpecs" na stránce 408 :

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

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

Související pojmy

"CipherSpecs a CipherSuites" na stránce 17

Kryptografické bezpečnostní protokoly musí souhlasit s algoritmem používaným 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
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 408

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 sebou samým na serveru AIX, Linux, and Windows” na stránce 287

Chcete-li požádat o digitální certifikát podepsaný certifikační autoritou pro produkční použití sady Suite B, viz “Požádání o osobní certifikát v systému AIX, Linux, and Windows” na stránce 290.

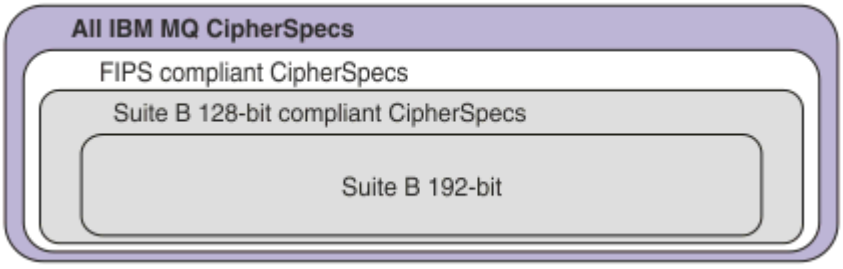
Poznámka: Používaná certifikační autorita musí generovat digitální certifikáty, které splňují požadavky popsané v IETF RFC 6460.

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" . Certifikát pro tento modul byl přesunut do historického stavu. Zákazníci by si měli prohlédnout IBM Crypto for C certificate a měli by si být vědomi jakýchkoli 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 41.

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 264

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 19. Další informace o konfiguraci Suite B a jejím vlivu na kanály TLS naleznete v části “Šifrování NSA Suite B v IBM MQ” na stránce 39.

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 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.
2. Nastavením proměnné prostředí MQSUITEB na jednu nebo více následujících hodnot:
   - ŽÁDNÉ
   - 128_BIT
   - 192_BIT

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

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

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

Úplné podrobnosti o struktuře MQSCO viz Volby konfigurace MQSCO-SSL.

Další informace o použití sady Suite B v konfiguračním souboru klienta viz Sekce SSL konfiguračního souboru klienta.

Další informace o použití proměnné prostředí MQSUITEB viz Popis proměnných prostředí.

.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 ověření platnosti certifikátu v produktu IBM MQ

Zásada ověření platnosti certifikátu určuje, jak přesně se validace řetězce certifikátů podřizuje odvětvovým standardům zabezpečení.

Zásada ověření platnosti certifikátu závisí na platformě a prostředí následujícím způsobem:

- Pro aplikace Java a JMS na všech platformách závisí zásada ověření platnosti certifikátu na komponentě JSSE běhového prostředí produktu Java . Další informace o zásadě ověření platnosti certifikátu naleznete v dokumentaci k vašemu prostředí JRE.
- Pro systémy IBM i závisí zásada ověření platnosti certifikátu na zabezpečené soketové knihovně poskytnuté operačním systémem. Další informace o zásadě ověření platnosti certifikátu naleznete v dokumentaci k operačnímu systému.
- Pro systémy z/OS závisí zásada ověření platnosti certifikátu na komponentě System SSL, kterou poskytuje operační systém. Další informace o zásadě ověření platnosti certifikátu naleznete v dokumentaci k operačnímu systému.
- Pro systémy AIX, Linux, and Windows je zásada ověření platnosti certifikátu dodána sadou GSKit a lze ji konfigurovat. Jsou podporovány dvě různé zásady ověření certifikátu:
  - Starší zásada ověření platnosti certifikátu, která se používá pro maximální zpětnou kompatibilitu a interoperabilitu se starými digitálními certifikáty, které nesplňují aktuální standardy ověření platnosti certifikátu IETF. Tato zásada je známá jako základní zásada.
  - Striktní, standardizovaná zásada ověření platnosti certifikátu, která vynucuje standard RFC 5280. Tato zásada je známá jako standardní zásada.

Informace o tom, jak nakonfigurovat zásadu ověření certifikátu v systému AIX, Linux, and Windows, viz “Konfigurace zásad ověřování certifikátů v adresáři IBM MQ” na stránce 42. Další informace o rozdílech mezi zásadami základního a standardního ověření certifikátu naleznete v tématu Ověřování platnosti certifikátu a návrh zásad důvěryhodnosti v produktu AIX, Linux, and Windows.

Konfigurace zásad ověřování certifikátů v adresáři IBM MQ

Můžete určit, která zásada ověření certifikátu TLS se používá k ověření digitálních certifikátů přijatých ze vzdálených partnerských systémů, a to čtyřmi způsoby.

Ve správci front lze zásadu ověření platnosti certifikátu nastavit následujícími způsoby:

- Použití atributu správce front *CERTVPOL*. Další informace o nastavení tohoto atributu viz ALTER QMGR.

Na klientovi existuje několik metod, které lze použít k nastavení zásady ověření platnosti certifikátu. Pokud je k nastavení zásady použita více než jedna metoda, klient použije nastavení v následujícím pořadí priorit:

1. Použití pole *CertificateValPolicy* ve struktuře MQSCO klienta. Další informace o použití tohoto pole naleznete v tématu Volby konfigurace MQSCO-SSL.
2. Pomocí proměnné prostředí klienta *MQCERTVPOL*. Další informace o použití této proměnné viz MQCERTVPOL.
3. Pomocí nastavení parametru ladění sekce SSL klienta *CertificateValPolicy*. Další informace o použití tohoto nastavení viz Sekce SSL konfiguračního souboru klienta.

Další informace o zásadách ověřování certifikátů naleznete v tématu “Zásady ověření platnosti certifikátu v produktu IBM MQ” na stránce 42.

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

V 9.2.0 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
2	ECDHE_RSA_	CipherSpecs , které používají veřejné klíče RSA, tajné klíče Elliptic Curve a algoritmy digitálního podpisu RSA.	RSA	RSA	ECDHE
V 9.2.0 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

V 9.2.0

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 39. 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 408
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 264
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 39
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 19
Vláda Spojených států amerických vyrábí technické poradenství v oblasti IT systémů a zabezpečení, včetně šifrování dat. Národní bezpečnostní agentura USA (NSA) doporučuje soubor interoperabilních šifrovacích algoritmů ve standardu Suite B.

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 jste právě začali s některými ukázkovými aplikacemi spuštěnými jako klienti, podívejte se na téma Příprava a spouštění ukázkových programů , kde najdete příklad nastavení správce front bezpečným pomocí záznamů ověření 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 ověření 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 určitých adres IP” na stránce 374.

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 376.

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 379.

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 378.

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 379.

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 380.

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 376.

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 377.

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 rozlišovacího jména SSL nebo TLS na ID uživatele MCAUSER" na stránce 378.

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 376.

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	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
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 94
Tento oddíl pojednává o aspektech zabezpečení vzdáleného systému zpráv.

Interakce se CHLAUTH a CONNAUTH

Jak probíhá interakce záznamů ověření kanálu (CHLAUTH) a ověření připojení (CONNAUTH) v produktu IBM MQ, v případě jedné konverzace na kanálu.

Různé typy vazeb

IBM MQ podporuje dvě metody pro připojení aplikace:

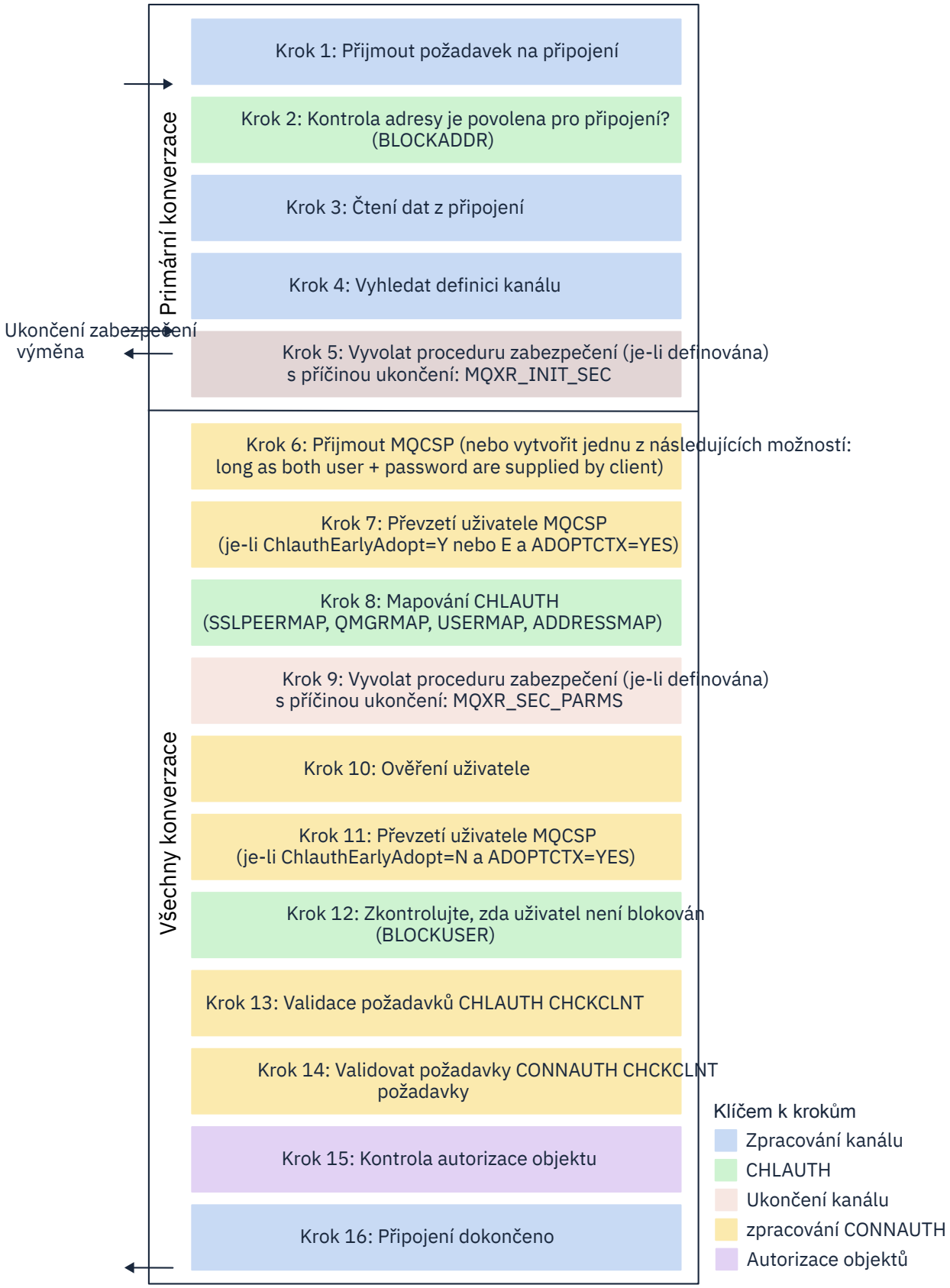
Lokální vazby
Platí, je-li aplikace a správce front na stejném operačním obrazu. CHLAUTH není důležitý pro tento typ připojení aplikace.

Vazby klienta
Používá se v případě, kdy aplikace a správce front používají síť ke komunikaci. Aplikaci a správce front lze spustit na stejném počítači, nebo mohou být na různých počítačích. V produktu IBM MQje připojení klienta ošetřeno ve formě kanálu SVRCONN (server-connection) a v této situaci jsou použitelné jak CONNAUTH, tak CHLAUTH.

Vázání kroků přijímajícího konce kanálu

Když se aplikace připojí ke správci front, provede se podstatné množství kontroly, které zajistí, že oba konce kanálu budou rozumět tomu, co je podporováno druhým koncem. Přijímající konec kanálu provádí některé další kontroly, zahrnující CHLAUTH a CONNAUTH, aby se zajistilo, že se klient může připojit, a tento proces může také zahrnovat ukončení zabezpečení, protože to může mít vliv na výsledek. Na tuto fázi připojení kanálu se odkazuje také jako na *fázi vázání*.

Následující diagram uvádí kroky, které kanál SVRCONN prochází při spuštění serveru (ve správci front):



Krok 1: Přijmout požadavek na připojení
Inicializátor kanálu nebo modul listener přijímá požadavek na připojení od jiného místa v síti.

Krok 2: Je povolena adresa pro připojení?
Před čtením dat produkt IBM MQ kontroluje adresu IP partnera proti pravidlům CHLAUTH a zjišťuje, zda se adresa nachází v pravidle *BLOCKADDR* . Pokud adresa nebyla nalezena, a proto není blokována, pokračuje tok do dalšího kroku.

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

Krok 4: Vyhledat definici kanálu
V prvním toku dat produkt IBM MQ odesílá mimo jiné název kanálu, který se odesílající konec pokouší spustit. Přijímající správce front poté může vyhledat definici kanálu, která má všechna nastavení uvedená pro daný kanál.

Krok 5: Odvolat proceduru zabezpečení (je-li definována)
Má-li kanál definovanou uživatelskou proceduru zabezpečení (SCYEXIT), je tato volba volána z důvodu uživatelské procedury (MQCXP.**ExitReason**) nastaven na hodnotu MQXR_INIT_SEC.

Krok 6: Přijetí MQCSP
Je-li to nutné, zkonstruujte jeden, dokud klient nedodává ID uživatele a heslo.

Je-li klientem aplikace Java nebo JMS se spuštěným v režimu kompatibility, klient nepředá strukturu MQCSP správci front. Místo toho, pokud aplikace dodala ID uživatele a heslo, struktura MQCSP se sestaví zde.

Krok 7: Převzetí uživatele MQCSP (pokud ChlauthEarlyAdopt je *Y* a ADOPTCTX=YES)
ID uživatele uplatněné klientem je ověřováno.

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

Je-li ověření úspěšné, ID uživatele je přijato kanálem a používá se v kroku mapování CHLAUTH.

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

Krok 8: Mapování CHLAUTH
Mezipaměť CHLAUTH se znovu zkontroluje, aby vyhledal pravidla mapování *SSLPEERMAP*, *USERMAP*, *QMGRMAP*a *ADDRESSMAP*.

Používá se pravidlo, které se shoduje s příchozím kanálem, který se nejvíce specificky používá. Pokud má pravidlo **USERSRC***(CHANNEL)* nebo *(MAP)*, bude kanál pokračovat ve vazbě.

Pokud se pravidla CHLAUTH vyhodnocují na pravidlo s **USERSRC***(NOACCESS)*, aplikace se zablokuje na připojení k kanálu, pokud nejsou pověření následně přepsána platným ID uživatele a heslem v kroku 9.

Krok 9: Zavolat proceduru zabezpečení (je-li definována)
Má-li kanál definovanou uživatelskou proceduru zabezpečení (SCYEXIT), je tato volba volána z důvodu uživatelské procedury (MQCXP.**ExitReason**) nastavte na hodnotu MQXR_SEC_PARMS.

Ukazatel na MQCSP bude přítomen v poli **SecurityParms** struktury MQCXP.

Struktura MQCSP má ukazatele na ID uživatele (MQCSP.**CSPUserIdPtr**) a heslo (MQCSP.**CSPPasswordPtr**).

Je možné změnit ID uživatele a heslo ve výstupu. 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 povědět IBM MQ pro zavření kanálu vrácením hodnoty *MQXCC_CLOSE_CHANNEL* v aplikaci MQCXP.Pole **Exitresponse** . Jinak bude zpracování kanálu pokračovat ve fázi ověření připojení.

Poznámka: Pokud je uplatněný uživatel změněn uživatelskou procedurou pro zabezpečení zprávy, pravidla mapování CHLAUTH nebudou znovu použita pro nového uživatele.

Krok 10: Ověření uživatele

Fáze ověření se provede, pokud je na správci front povoleno CONNAUTH.

Chcete-li tuto kontrolu 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 .

Jako ověření operačního systému (**AUTHTYPE**(*IDPWOS*)) platí jak pro IBM MQ for Multiplatforms , tak pro IBM MQ for z/OS, příklady používají ověření operačního systému.

z/OS Následující příklad ukazuje zaslaný výchozí objekt pro **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 zaslaný výchozí objekt pro **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)
```

Typ AUTHINFO TYPE (IDPWOS) má atribut nazvaný CHCKCLNT. Je-li hodnota změněna na *REQUIRED* , všechny klientské aplikace musí dodat platné ID uživatele a heslo.

Pokud byl uživatel ověřen v kroku 7, nebude uživatel znovu ověřen, dokud nebude uživatel nebo heslo v poli SecurityParms struktury MQCXP změněno uživatelskou procedurou zabezpečení v kroku 9.

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

Pokud bylo ID uživatele deklarováno v objektu MQCSP nebo pole **`SecurityParms`** struktury MQXCP úspěšně ověřeno a **ADOPTCTX** je *YES*, bude kontext uživatele, který je výsledkem kroků 7 a 8 , přijat jako kontext, který má být použit pro tuto aplikaci, pokud nebyl uživatel nebo heslo v poli **`SecurityParms`** struktury MQCXP změněno uživatelskou procedurou zabezpečení v kroku 9.

Toto deklarovaný ID uživatele je ID uživatele, které je zkontrolováno pro autorizaci k použití prostředků produktu IBM MQ .

Například, v kanálu SVRCONN nemáte nastaven parametr MCAUSER a klient běží pod '`johndoe`' na počítači se systémem Linux . Vaše aplikace určuje uživatele '`fred`' v objektu MQCSP, takže kanál začíná běžet s hodnotou '`johndoe`' jako aktivní MCAUSER. Po kontrole CONNAUTH se přijme uživatel '`fred`' a kanál se spustí s '`fred`' jako aktivním MCAUSER.

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

Step13: Ověřte požadavky CHLAUTH CHCKCLNT
Pokud pravidlo CHLAUTH, které bylo zvoleno v kroku 8 , navíc uvádí hodnotu CHCKCLNT, nebo REQDADM, pak se provede ověření platnosti, aby bylo zajištěno, že bylo poskytnuto platné ID uživatele CONNAUTH, aby bylo možné splnit požadavek.

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

Notes:

1. Je-li nastavena hodnota CHCKCLNT (REQUIRED) nebo CHCKCLNT (REQDADM), ale CONNAUTH není ve správci front povoleno, připojení selže s návratovým kódem MQRC_SECURITY_ERROR (2063) kvůli konfliktu v konfiguraci.
2. V tomto kroku není uživatel znovu ověřen.

Krok 14: Validovat požadavky CONNAUTH CHCKCLNT.
Fáze ověření se provede, pokud je na správci front povoleno CONNAUTH.

Hodnota CONNAUTH CHCKCLNT se kontroluje, aby se určilo, jaké požadavky jsou nastaveny pro příchozí připojení:

- Je-li nastaven parametr CHCKCLNT (NONE), bude tento krok vynechán.
- Je-li nastaven parametr CHCKCLNT (OPTIONAL), tento krok se přeskočí.
- Je-li nastavena hodnota CHCKCLNT (REQUIRED), musí být uživatel ověřen v kroku 7 nebo 10. Jinak se připojení odmítne.
- Je-li nastavena hodnota CHCKCLNT (REQDADM), musí být uživatel ověřen v kroku 7 nebo 10 , je-li toto připojení určeno pro privilegované uživatele. Jinak se připojení odmítne.

Poznámka: V tomto kroku není uživatel znovu ověřen.

Multi **Krok 15: Kontrola oprávnění k objektu**
Je provedena kontrola, aby se zajistilo, že aktivní MCAUSER má odpovídající oprávnění pro připojení ke správci front.

ALW Další informace viz Object Authority Manager.

IBM i Další informace viz “Správce oprávnění objektu v systému IBM i” na stránce 152.

Krok 16: Připojení dokončeno
Pokud byly předchozí kroky úspěšně dokončeny, připojení bude dokončeno.

Související pojmy
CONNAUTH
Správce front lze konfigurovat tak, aby používal zadané ID uživatele a heslo ke kontrole, zda má uživatel oprávnění pro přístup k prostředkům.

Související odkazy
SET CHLAUTH
ZMĚNIT AUTHINFO

Řešení problémů přístupu CHLAUTH
Návrhy, jak řešíte určité problémy s přístupem při použití záznamů ověření kanálu (CHLAUTH).

Výchozí pravidla CHLAUTH

Pro zpracování CHLAUTH existují tři výchozí pravidla:

- ŽÁDNÝ PŘÍSTUP ke všem kanálům všemi uživateli produktu `MQ-admin*`
- NENÍ PŘÍSTUP k frontě SYSTEM.* kanály pro všechny uživatele
- POVOLIT přístup k SYSTEM.ADMIN.SVRCONN kanál (jiné než `MQ-admin` uživatelé)

První dvě pravidla blokují přístup ke všem kanálům. Třetí pravidlo je více specifické, a proto má přednost před ostatními dvěma, je-li kanál SYSTEM.ADMIN.SVRCONN , čímž je povolen přístup k tomuto kanálu.

Běžné chyby připojení

Pravidla CHLAUTH se používají k určení, zda lze kanál spustit, a které umožňují mapování přes MCAUSER na jiné ID uživatele. Pokud kanál nelze spustit, často se vyskytují 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 blokován.
- MQJE001: Došlo k výjimce MQException: Kód dokončení 2, důvod 2035
- MQJE036: Pokus o připojení správce front byl odmítnut.

Měli byste blokovat přístup přísně, pak přidat další pravidla CHLAUTH pravidla pro ovládání, kdo může přistupovat a spustit kanály. Jako dočasné opatření a pro odstraňování chyb uvedených v seznamu můžete:

- “Zakázat pravidla CHLAUTH” na stránce 58
- “Upravit nebo odebrat pravidla CHLAUTH” na stránce 59

Zakázat pravidla CHLAUTH

Jako dočasné opatření a také pro odstraňování chyb výše uvedených chyb můžete zakázat pravidla CHLAUTH. Pravidla lze kdykoli znovu povolit a v případě zakázání pravidel CHLAUTH dojde k vyřešení problému s připojením, víte, že to byla příčina.

Chcete-li zakázat pravidla CHLAUTH, zadejte následující příkaz:

```
runmqsc: ALTER QMGR CHLAUTH (DISABLED)
```

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

Upravit nebo odebrat pravidla CHLAUTH

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

Chcete-li upravit pravidlo CHLAUTH, použijte příkaz SET CHLAUTH spolu s ACTION (REPLACE). Chcete-li například upravit výchozí pravidlo, které nezpůsobuje přístup ke všem kanálům žádným uživatelům produktu `MQ-admin` na hodnotu WARN (namísto blokování), zadejte následující příkaz:

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

Chcete-li odstranit pravidlo CHLAUTH, použijte příkaz SET CHLAUTH s ACTION (REMOVE). Chcete-li například odstranit výchozí pravidlo, které nezpůsobuje žádný přístup ke všem kanálům libovolnými uživateli produktu `MQ-admin` , zadejte následující příkaz:

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

Testování přístupu pomocí MATCH (RUNCHECK)

Výsledek vašich pravidel CHLAUTH můžete testovat pomocí volby MATCH (*RUNCHECK*) pravidla CHLAUTH v runmqsc. Volba **MATCH** (*RUNCHECK*) vrátí záznam, který se shoduje s konkrétním příchozím kanálem za běhu, pokud se tento kanál připojuje k tomuto správci front. Musíte zadat:

- Název kanálu
- atribut Adresa
- Atribut SSLPEER, pouze v případě, že příchozí kanál používá zabezpečení SSL nebo TLS
- QMNAME, je-li příchozí kanál kanál správce front, nebo
- Atribut CLNTUSER, je-li příchozí kanál kanálem klienta

Následující příklad zkontroluje, jaké pravidlo CHLAUTH, s výchozími pravidly na místě, vede k přístupu uživatele `MQ-admin` `johndoe` k kanálu s názvem `CHAN1`:

```
runmqsc: 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`, kanál se nespustí, uživatel bude zablokován kvůli pravidlu BLOCKUSER pro uživatele *MQADMIN.

Následující příklad zkontroluje, jaké pravidlo CHLAUTH, s výchozími pravidly na místě, má za následek uživatele `alice` , který není uživatelem `MQ-admin` a má přístup ke kanálu s názvem `CHAN1`:

```
runmqsc: 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, které se používá ke kontrole oprávnění k objektu IBM MQ .

Související odkazy

SET CHLAUTH

ZOBRAZIT VELIKOST CHUSH

Vytvoření nového pravidla CHLAUTH pro uživatele

Některé běžné scénáře pro uživatele, a příklad pravidla CHLAUTH k dosažení těchto.

Toto téma obsahuje následující scénáře:

- “Řízení přístupu pro specifické uživatele produktu MQ-admin” na stránce 60
- “Řízení přístupu pro konkrétní uživatele a aplikaci klienta IBM MQ” na stránce 61
- “Řízení přístupu pro specifického uživatele pomocí rozlišovacího jména (DN) certifikátu tohoto uživatele” na stránce 61
- “Mapování konkrétního uživatele na uživatele produktu mqm” na stránce 62

Řízení přístupu pro specifické uživatele produktu MQ-admin

Pro tento scénář nastavte kanál připojení serveru, který má být použit výhradně pro administrativní perspektivu, tj. pro připojení z produktu IBM MQ Explorer. Pro toto použití máte specifický kanál a definovanou adresu IP nebo adresy, z nichž chcete připojení přijmout, a přístup blokovaný pro ID `'mqm'` , pokud připojení není z jedné z uvedených adres IP.

Učinit kanál SVRCONN pro uživatele IBM MQ Explorer a `MQ-admin` s názvem `ADMIN.CHAN`:

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

Pro testování se ujistěte, že máte definovánu uživatele, který je ve skupině `MQ-admin` , a ten, který není. Pro tento scénář platí, že `mqadm` je ve skupině `MQ-admin` a `alice` není.

Výchozí pravidla CHLAUTH jsou na místě. Přidejte tři pravidla, která umožní specifickému uživateli přistoupit k ADMIN.CHAN jako `MQ-admin` z určitých adres IP:

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

```
runmqsc:
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 okamžiku může uživatel `mqadm` přistoupit a spustit ADMIN.CHAN channel, z uvedeného rozsahu IP adres.

MATCH (RUNCHECK) můžete spustit kdykoli a zobrazit výsledky každého z těchto příkazů:

```
runmqsc:
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 okamžiku pouze uživatelé, kteří mají záznam CHLAUTH, mají povolen přístup k použití ADMIN.CHAN.

Řízení přístupu pro konkrétní uživatele a aplikaci klienta IBM MQ

Pro tento scénář platí, že výchozí pravidla CHLAUTH jsou adekvátní, předpokládá se, že oprávnění IBM MQ bude nastaveno pro specifického uživatele, aby poskytl správné oprávnění IBM MQ (pomocí příkazu setmqaut).

V tomto scénáři jsou oprávnění nastavena pro uživatele `mqapp1`, který není uživatelem produktu `MQ-admin` . Učinit kanál SVRCONN, APP1.CHAN-použije se konkrétní aplikace a specifický uživatel.

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

S parametrem default CHLAUTH rules na místě může uživatel `mqapp1` spustit APP1.CHAN .

ID uživatele, které pochází z aplikace klienta IBM MQ , se používá pro kontrolu oprávnění k objektu IBM MQ . V tomto případě za předpokladu, že uživatel 'mqapp1' spouští aplikaci klienta IBM MQ , se používá pro kontrolu oprávnění k objektu produktu IBM MQ . Proto, pokud má produkt `mqapp1` přístup k objektům produktu IBM MQ , které aplikace potřebuje, je vše v pořádku; pokud se nejedná o chyby oprávnění, získáte chyby oprávnění.

Můžete dále zvýšit zabezpečení vytvořením specifických pravidel CHLAAUTH pro ID uživatele produktu `mqapp1` , ale podle výchozích pravidel nemá žádný člen skupiny `MQ-admin` přístup k tomuto kanálu.

```
runmqsc:
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 rozlišovacího jména (DN) certifikátu tohoto uživatele

Pro tento scénář musí mít uživatel k témuž správci front certifikát, který je do toku správce front. DN se pak porovnává s nastavením pravidla SSLPEER pravidla CHLAUTH a SSLPEER může používat zástupné znaky.

Je-li nalezena shoda, může být uživatel také mapován na jinou MCAUSER pro účely kontroly oprávnění k objektům IBM MQ . Mapování MCAUSER může minimalizovat počet uživatelů, kteří musí být spravováni ve správci oprávnění objektu IBM MQ (OAM).

Máte kanál TLS s certifikáty, které se používají, a požadujete pravidla pro:

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

```
.
# 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 k kanálu, se používá pro oprávnění IBM MQ OAM objektů IBM MQ . Proto musí mít ID uživatele příslušné oprávnění IBM MQ .

Můžete mapovat na odlišné ID uživatele produktu IBM MQ , pokud chcete, pomocí:

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

místo USERSRC(CHANNEL).

Mapování konkrétního uživatele na uživatele produktu mqm

Jedná se o přidání nebo úpravu produktu “Řízení přístupu pro specifické uživatele produktu MQ-admin” na stránce 60.

Přidejte následující pravidlo CHLAUTH, chcete-li mapovat konkrétní uživatele na uživatele produktu mqm nebo ID uživatele produktu MQ-admin , který má nastavení oprávnění k objektu IBM MQ v produktu IBM MQ OAM.

```
runmqsc:
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 namapuje uživatele johndoe na uživatele mqm pro konkrétní kanál ADMIN.CHAN.

Související pojmy

“Řešení problémů přístupu CHLAUTH” na stránce 58
Návrhy, jak řešíte určité problémy s přístupem při použití záznamů ověření kanálu (CHLAUTH).

“Vytvoření nového pravidla CHLAUTH pro kanály” na stránce 62
Chcete-li vám pomoci vytvořit vlastní pravidla CHLAUTH, zde jsou některé běžné scénáře pro kanály, a příklad CHLAUTH pravidel k provedení těchto.

Související odkazy

SET CHLAUTH

ZOBRAZIT VELIKOST CHUSH

Vytvoření nového pravidla CHLAUTH pro kanály

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

Toto téma obsahuje následující scénáře:

- “Povolit přístup pouze ke konkrétnímu kanálu ze specifického rozsahu adres IP.” na stránce 62
- “Pro specifický kanál blokujte všechny uživatele, ale umožněte, aby se připojili ke specifickým uživatelům.” na stránce 63
- “Použití CHLAUTH pro kanály příjemce a odesílatele” na stránce 63

Povolit přístup pouze ke konkrétnímu kanálu ze specifického rozsahu adres IP.

Pro tento scénář chcete provést následující akce:

- Nastavení Bez přístupu ke kanálu odkudkoli
- Povolit přístup ze specifické 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 se má spustit, když připojení pochází ze specifikovaného rozsahu IP adres.

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

Pro specifický kanál blokujte všechny uživatele, ale umožněte, aby se připojili ke specifickým uživatelům.

V případě tohoto scénáře má přístup k kanálu MY.SVRCONN výchozí nastavení 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 kohokoli z připojení na MY.SVRCONN, pak kód umožňuje spustit pouze kanál MY.SVRCONN , když připojení pochází ze specifického ID uživatele `johndoe`.

Uživatel, který se připojuje k kanálu `johndoe` , se používá pro oprávnění OAM produktu IBM MQ pro objekty IBM MQ . Proto musí mít ID uživatele příslušné oprávnění IBM MQ .

Můžete mapovat na odlišné ID uživatele produktu IBM MQ , pokud chcete, pomocí:

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

místo `USERSRC(CHANNEL)`.

Použití CHLAUTH pro kanály příjemce a odesílatele

Pomocí pravidel CHLAUTH můžete přidat další zabezpečení k přijímači a odesílatelům kanálů, a omezit tak přístup k přijímacímu kanálu. Všimněte si, že pokud přidáváte nebo provádíte změny pravidel CHLAUTH, aktualizovaná pravidla CHLAUTH se použijí pouze při spouštění kanálu, takže pokud jsou kanály již spuštěny, je třeba je zastavit a restartovat, aby se aplikovaly aktualizace CHLAUTH.

Pravidla CHLAUTH mohou být použita na libovolném kanálu, ale existují určitá omezení. Např. pravidla USERMAP se vztahují pouze na kanály SVRCONN.

Tento příklad umožňuje připojení pouze z určité IP adresy, aby se spustil TO.MYSVR1 kanál:

```
# 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 pojmy

“Řešení problémů přístupu CHLAUTH” na stránce 58
Návrhy, jak řešíte určité problémy s přístupem při použití záznamů ověření kanálu (CHLAUTH).

“Vytvoření nového pravidla CHLAUTH pro uživatele” na stránce 59

Některé běžné scénáře pro uživatele, a příklad pravidla CHLAUTH k dosažení těchto.

Související odkazy
SET CHLAUTH
ZOBRAZIT VELIKOST CHUSH

Vytvoření pravidla back-stop CHLAUTH
Když přemýšlíte o řízení příchozích připojení do svého správce front, máte dvě možnosti. Buď se můžete pokusit zobrazit seznam všech spojení, která nejsou dovolena, nebo můžete začít tím, že budete říkat všechna spojení, která nejsou povolena, a pak se pokuste vypsat všechna povolená spojení. Tato druhá volba je zde popsána.

Informace o této úloze

Důvodem použití druhé volby je, že pokud se pokusíte vypsat všechna připojení, která nejsou povolena, a vše, co není uvedeno, je proto povoleno v tom, že v důsledku chybějícího seznamu je připojení, které by nemělo být povoleno, se může připojit, což může způsobit narušení zabezpečení.

Naopak, pokud místo toho začnete tím, že každé připojení není povoleno, a pak seznam těch, které jsou, výsledkem toho, že tento seznam chybí, není narušení zabezpečení. Pokud váš podnik vyžaduje přidání dalších připojení, jedná se o relativně jednoduchou úlohu, ale neexistuje žádné potenciální narušení zabezpečení.

Prvním krokem je vytvoření pravidla *back-stop* , což je pravidlo, které zachytil všechna připojení, která nejsou jinak porovnána s více specifickými pravidly. Toto pravidlo má za následek zastavení jakýchkoli vzdálených připojení, aby bylo možné připojit se k vašemu správci front vůbec.

Pokud se však o tento přístup zajímá, můžete nastavit pravidlo *back-stop* ve varovném režimu; viz krok “2” na stránce 64

Postup

1. Chcete-li vytvořit pravidlo zpětného zastavení, 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 zavřel dveře na všech vzdálených připojeních, můžete začít tím, že uvedete více specifických pravidel, která umožní určitá spojení. 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 provést všechna vaše pozitivní pravidla. Pokud se domníváte, že jste vytvořili všechna potřebná pravidla, zapněte události kanálu zadáním následujícího příkazu:

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

   a monitorujte server SYSTEM.ADMIN.CHANNEL.EVENT pro události s **Reason** nastaveným na MQRC_CHANNEL_BLOCKED_WARNING.

   Tyto události podrobně popisují připojení, která porovnávají vaše pravidlo zpětného zastavení, ale protože příkaz běží ve varovném režimu, nebyl ve skutečnosti zablokován pro tuto chvíli.

Přezkoumejte každou z těchto událostí a určete, zda má toto připojení obsahovat kladné pravidlo, zda je v něm povoleno, nebo zda se správně shoduje s pravidlem *back-stop* . Můžete pracovat v tomto režimu, přezkoumat události tak, jak jsou vytvořeny, dokud nebudete spokojeni, že jste viděli všechny příchozí kanály, a máte pro ně vhodná pozitivní pravidla.

V tomto bodě můžete změnit pravidlo *back-stop* a začít opravdu blokovat připojení, která se shodují, zadáním následujícího příkazu:

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

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

Informace o této úloze

V kontextu této úlohy platí následující podmínky:

oprávněný uživatel
Uživatel, který má oprávnění k provedení operace bez explicitního udělení přístupu k provedení této operace. Příkladem těchto privilegovaných uživatelů jsou uživatelé ve skupině mqm.

IBM MQ administrátor
Uživatel, který má potřebu vydávat administrativní příkazy vůči produktu IBM MQ, jako například **DEFINE QLOCAL** nebo **START CHANNEL**.

Následující kroky vytvářejí neprivilegovaného administrátora produktu IBM MQ .

Postup

1. Vytvořte ID uživatele na počítači správce front s použitím 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 produktu IBM MQ provedením následujícího postupu:
   a) Spusťte produkt IBM MQ Explorer pomocí privilegovaného uživatele.
   b) Přejděte do *Průvodce na základě role* tak, že vyberete odpovídajícího správce front, poté `Oprávnění k objektu` a `Přidat oprávnění založená na rolích`.
   c) Na panelu průvodce, který se objeví, zadejte ID uživatele, které jste vytvořili v prvním kroku, nebo pokud dáváte přednost práci se skupinami, zadejte jméno skupiny pro uživatele nebo sadu uživatelů, které chcete provést v neprivilegovaných administrátorů produktu IBM MQ .
   d) Nastavte průvodce pro úplný administrativní přístup.
   e) Chcete-li povolit, aby váš neprivilegovaný administrátor produktu IBM MQ mohl být schopen procházet zprávy ve frontách, zaškrtněte toto políčko.
   f) Zkontrolujte příkazy na panelu náhledu v dolní části průvodce.

      Tyto příkazy můžete vyjmout a vložit, chcete-li sestavit vlastní skripty.

      Jedním z důvodů, proč můžete raději dělat to s vaším vlastním skriptem, je snížit množství přístupu, které poskytujete tomuto uživateli. Možná raději udělíte přístup ke všem objektům, ale raději udělíte přístup pouze k určité skupině objektů.

      Po stisknutí tlačítka **OK** v průvodci se zobrazí příkazy tak, jak jsou zobrazeny.
   g) Chcete-li povolit vzdálený přístup pro toto ID uživatele, musíte nastavit některá pravidla CHLAUTH, pokud má být požadavek na neprivilegovaného administrátora produktu IBM MQ určen také pro vzdálený přístup.

      Předpokládejme, že váš podnik používá v produktu “Vytvoření pravidla back-stop CHLAUTH” na stránce 64pokyny, vše, co potřebujete, je přidat pravidlo, které umožňuje toto pravidlo.

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

Používáte-li slabé ověření TCP/IP, můžete nastavit pravidlo CHLAUTH, které bude vypadat 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 TLS ověření, můžete nastavit pravidlo CHLAUTH, které bude vypadat takto:

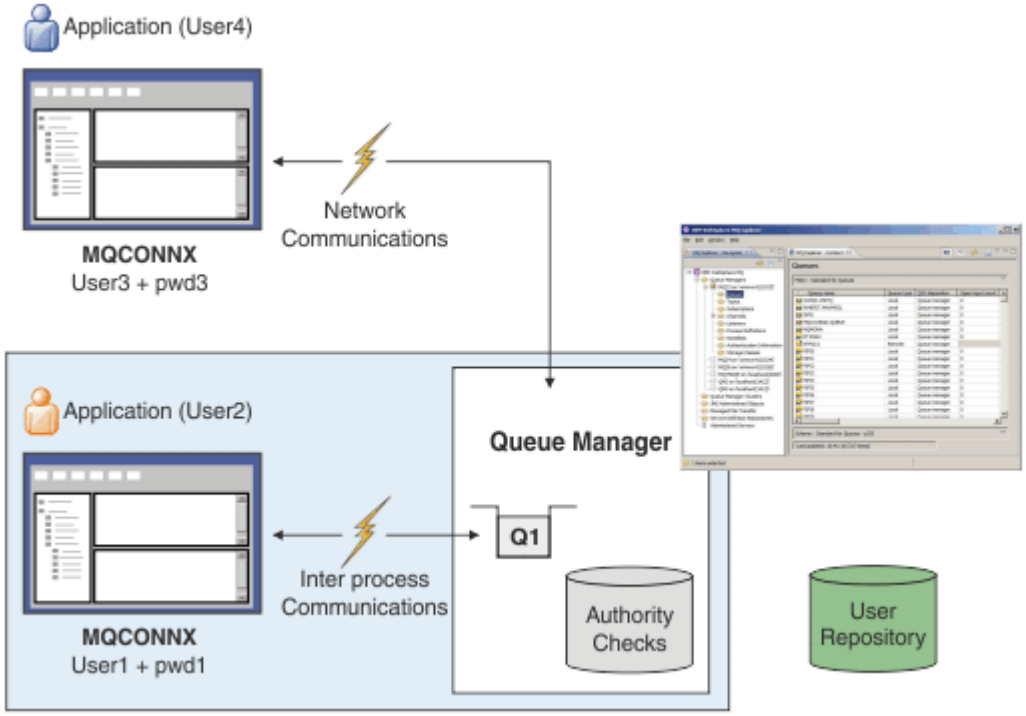
```
SET CHLAUTH(admin-channel-name)      TYPE(SSLPEERMAP)
SSLPEER('CN=Alice') ADDRESS('1.2.3.4')      USERSRC(MAP) MCAUSER('alice')
DESCR('Admin Channel - TLS authentication'
```

Nyní, když se uživatel připojí do `admin-channel-name` (a odpovídá pravidlům CHLAUTH), je schopen vydávat příkazy pod ID uživatele `alice` ve správci front, a tak privilegovaný vzdálený přístup není požadován.

Ověření připojení

Ověření připojení může být dosaženo různými způsoby:

- Aplikace může poskytnout ID uživatele a heslo. Aplikace může být buď klientem, nebo může používat lokální vazby.
- Správce front může být konfigurován tak, aby se choval na základě zadaného ID uživatele a hesla.
- Úložiště lze použít k určení, zda je kombinace ID uživatele a hesla platná.



V diagramu se dvě aplikace vytváří připojení ke správci front, jedna aplikace jako klient a jedna s použitím lokálních vazeb. Aplikace mohou používat nejrůznější rozhraní API pro připojení ke správci front, ale všechny mají schopnost poskytnout 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 poskytovaného aplikací, `User1` a `User3`.

Správce front obdrží konfigurační příkazy (v diagramu IBM MQ Explorer se používá) a spravuje otevírání prostředků a kontroluje oprávnění k přístupu k těmto prostředkům. V produktu IBM MQ existuje mnoho

různých prostředků, ke kterým může aplikace vyžadovat přístup oprávnění. Diagram ilustruje otevření fronty pro výstup, ale stejné zásady platí i pro ostatní prostředky.

Podrobnosti o úložišti používaném pro kontrolu ID uživatelů a hesel najdete v tématu Uživatelská úložiště .

Související pojmy

“Ověření připojení: Konfigurace” na stránce 67
Správce front lze konfigurovat tak, aby používal zadané ID uživatele a heslo ke kontrole, zda má uživatel oprávnění pro přístup k prostředkům.

“Ověření připojení: Změny aplikace” na stránce 71

“Ověření připojení: Úložiště uživatelů” na stránce 72
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 konfigurovat tak, aby používal zadané ID uživatele a heslo ke kontrole, zda má uživatel oprávnění pro přístup k prostředkům.

Zapnutí ověřování připojení ve správci front

V objektu správce front lze atribut **CONNAUTH** nastavit na název objektu ověřovacích informací (AUTHINFO). Tento objekt může být jedním ze dvou typů (atribut AUTHTYPE):

IDPWOS
Označuje, že správce front používá lokální operační systém k ověření ID uživatele a hesla.

IDPWLDAP
Označuje, že správce front používá server LDAP k ověření ID uživatele a hesla.

Poznámka: V poli **CONNAUTH** nemůžete použít žádný jiný typ objektu ověřovacích informací.

IDPWOS a IDPWLDAP jsou podobné v řadě svých atributů, které jsou popsány zde. Další atributy jsou zvažovány později.

Chcete-li zkontrolovat lokální připojení, použijte atribut AUTHINFO **CHCKLOCL** (zkontrolujte lokální připojení). Chcete-li zkontrolovat připojení klienta, použijte atribut AUTHINFO **CHCKCLNT** (zkontrolujte připojení klienta). Před rozpoznáním změn správcem front je nutné aktualizovat konfiguraci.

```
ALTER QMGR CONNAUTH(USE.PW)
DEFINE AUTHINFO(USE.PW) +
AUTHTYPE(IDPWOS) +
FAILDLAY(10) +
CHCKLOCL(OPTIONAL) +
CHCKCLNT(REQUIRED)
REFRESH SECURITY TYPE(CONNAUTH)
```

Kde USE.PW v CONNAUTH je řetězec, který odpovídá definici AUTHINFO.

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

NONE
Vypne kontrolu.

Volitelný
Zajišťuje, že pokud je ID uživatele a heslo poskytnuto aplikací, jedná se o platnou dvojici, ale není povinné je poskytovat. Tato volba může být užitečná například během migrace.

Důležité: VOLITELNĚ je minimální hodnota, kterou můžete nastavit, aby bylo možné použít přísnější pravidla CHLAUTH.

Pokud vyberete NONE a připojení klienta odpovídá záznamu CHLAUTH s CHCKCLNT 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.

POVINNÉ
Vyžaduje, aby všechny aplikace poskytovaly platné ID uživatele a heslo. Viz také následující poznámka.

REQDADM
Oprávnění uživatelé musí zadat platné ID uživatele a heslo, 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 **CHCKLOCL** na hodnotu REQUIRED nebo REQDADM znamená, že správce front nelze lokálně spravovat pomocí **runmqsc** (chyba AMQ8135: Neautorizováno), pokud uživatel nezadá parametr -u UserId na příkazovém řádku **runmqsc** . S touto sadou produkt **runmqsc** vyzve k zadání hesla uživatele na konzole.

Podobně se uživateli, který spouští průzkumník IBM MQ Explorer v lokálním systému, při pokusu o připojení ke správci front zobrazí chyba AMQ4036 . Chcete-li zadat jméno 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 jméno uživatele a heslo, které se má použít, a poté klepněte na tlačítko **OK**.

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

Parametr **CONNAUTH** je prázdný pro migrované správce front, ale je nastaven na hodnotu *SYSTEM.DEFAULT.AUTHINFO.IDPWOS* pro nové správce front. Předchozí definice **AUTHINFO** má standardně nastavenu hodnotu **CHCKCLNT** na *REQDADM* .

Proto musíte poskytnout správné heslo operačního systému pro všechny existující klienty, kteří pro připojení používají ID oprávněného uživatele.

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 aplikace klienta odpovídajícím způsobem chráněna, prohlédněte si téma “Ochrana heslem MQCSP” na stránce 29.

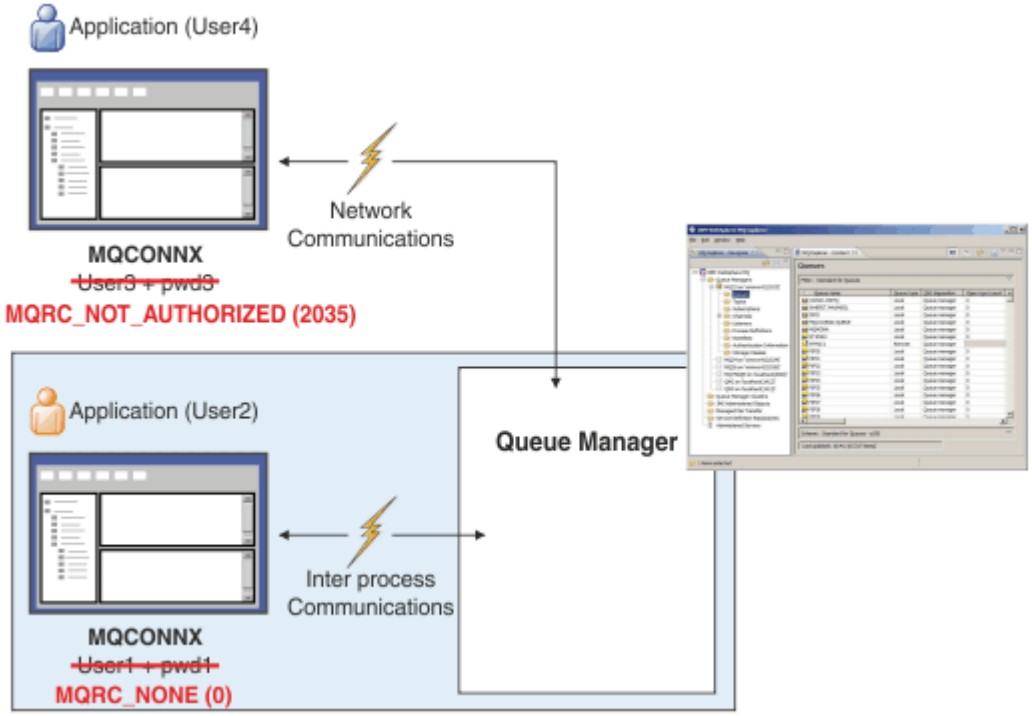
Granularita konfigurace

Kromě **CHCKLOCL** a **CHCKCLNT** , které se používají k zapnutí kontroly ID uživatele a hesla, existují vylepšení pravidel CHLAUTH , aby bylo možné provést specifičtější konfiguraci pomocí **CHCKCLNT**.

Můžete například nastavit celkovou hodnotu **CHCKCLNT** na VOLITELNĚa poté ji upgradovat na přísnější nastavení pro určité kanály nastavením parametru **CHCKCLNT** na hodnotu REQUIRED nebo REQDADM v pravidle CHLAUTH . Standardně se pravidla CHLAUTH spustí s CHCKCLNT(ASQMGR) , takže se tato granularita nemusí používat. Příklad:

```
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)
```

Oznámení o chybě



Pokud aplikace v případě potřeby nedodá ID uživatele a heslo nebo dodá nesprávnou kombinaci, i když je volitelná, dojde k chybě.

Poznámka: Když je kontrola hesla vypnuta pomocí volby NONE na **CHCKLOCL** nebo **CHCKCLNT**, neplatná hesla nejsou zjištěna.

Nezdařená ověření jsou zadržena po dobu v sekundách určenou atributem **FAILDLAY** , než je chyba vrácena aplikaci. To poskytuje určitou ochranu před aplikací, která se opakovaně pokouší o připojení.

Chyba je zaznamenána několika způsoby:

Aplikace
Aplikaci je vrácena standardní chyba zabezpečení IBM MQ , RC2035 -MQRC_NOT_AUTHORIZED.

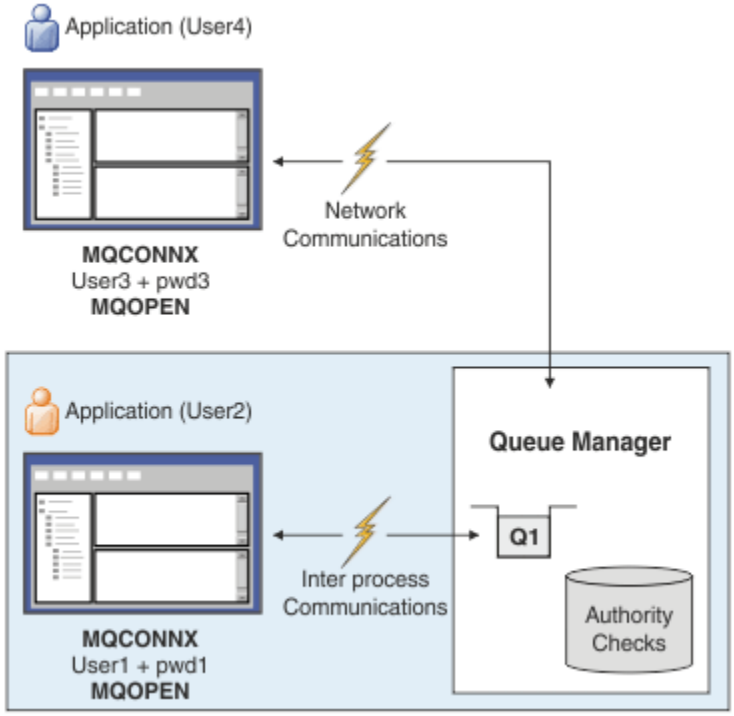
Administrátor
Administrátor systému IBM MQ vidí událost hlášenou v protokolu chyb, a proto může vidět, že aplikace byla odmítnuta, protože ID uživatele a heslo neprošlo kontrolou, a ne proto, že například neexistovalo žádné oprávnění k připojení .

Nástroj pro monitorování
Nástroj monitorování může být také upozorněn na selhání, pokud zapnete události oprávnění odesláním zprávy události do SYSTEM.ADMIN.QMGR.EVENT fronta:

```
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. Heslo není uvedeno ve zprávě události. To znamená, že ve zprávě události jsou dvě ID uživatele: ID, pod kterým je aplikace spuštěna, a ID, které aplikace prezentovala pro kontrolu ID uživatele a hesla.

Relace k autorizaci



Můžete nakonfigurovat správce front tak, aby pověřil, aby určité aplikace poskytovaly ID uživatele a hesla, protože ID uživatele, pod kterým je aplikace spuštěna, nemusí být stejné ID uživatele, které aplikace předložila spolu s heslem, když aplikace otevře frontu pro výstup, například:

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

Způsob zpracování ID uživatelů a hesel je řízen atributem **ADOPTCTX** na objektu ověřovacích informací.

POKUD CTX (ANO)
Všechny kontroly autorizace pro aplikaci jsou provedeny se stejným ID uživatele, které jste ověřili pomocí hesla, výběrem převzetí kontextu jako kontext aplikace po zbytek životnosti připojení.

Upozornění: Používáte-li ID uživatele pro systém souborů (YES) a OS, musíte se ujistit, že adoptované ID uživatele nepřekračuje maximální délku ID uživatele. Další informace viz “ID uživatelů” na stránce 82.

ADOPTCTX (NO)
Aplikace poskytuje ID uživatele a heslo pro účely jejich ověření v době připojení, ale pak pokračuje s použitím ID uživatele, pod kterým je aplikace spuštěna 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).

Upozornění:

Když použijete parametr **ADOPTCTX(YES)** na objektu ověřovacích informací, nemůže být převzat jiný kontext zabezpečení, pokud nenastavíte parametr **ChlauthEarlyAdopt** v sekci kanálů souboru `qm.ini` .

Výchozí objekt ověřovacích informací je například nastaven na hodnotu **ADOPTCTX(YES)** a uživatel `fred` je přihlášen. Jsou nakonfigurována následující dvě pravidla CHLAUTH:

```
SET CHLAUTH('MY.CHLAUTH') TYPE(ADDRESSMAP) DESCR('Block all access by
default') ADDRESS('*') USERSRC(NOACCESS) ACTION(REPLACE)
SET CHLAUTH('MY.CHLAUTH') TYPE(USERMAP) DESCR('Allow user bob and force
CONNAUTH') CLNTUSER('bob') CHCKCLNT(REQUIRED) USERSRC(CHANNEL)
```

Je vydán následující příkaz s úmyslem ověřit příkaz jako přijatý kontext zabezpečení uživatele bob:

```
runmqsc -c -u bob QMGR
```

Správce front ve skutečnosti používá kontext zabezpečení `fred`, nikoli bob, a připojení se nezdaří.

Další informace o produktu **ChlauthEarlyAdopt** naleznete v tématu Atributy sekce kanálů.

Související pojmy

“Ověření připojení” na stránce 66

“Ověření připojení: Změny aplikace” na stránce 71

“Ověření připojení: Úložiště uživatelů” na stránce 72

Pro každého z vašich správců front můžete zvolit různé typy objektů ověřovacích informací pro ověřování ID uživatelů a hesel.

Ověření připojení: Změny aplikace

Aplikace může v rámci struktury parametrů zabezpečení připojení (MQCSP) zadat ID uživatele a heslo, je-li volána funkce MQCONNX. ID uživatele a heslo jsou předány ke kontrole na správce oprávnění k objektu (OAM) dodaném se správcem front nebo komponenta autorizační služby dodaná se správcem front v systémech z/OS . Nemusíte psát své vlastní uživatelské rozhraní.

Je-li aplikace spuštěna jako klient, je ID uživatele a heslo předáno také do uživatelských procedur zabezpečení na straně klienta a na straně serveru pro zpracování. Lze je také použít pro nastavení atributu ID uživatele agenta kanálu zpráv (MCAUSER) instance kanálu. Uživatelská procedura zabezpečení je volána z důvodu ukončení MQXR_SEC_PARMS pro toto zpracování. Uživatelské procedury zabezpečení na straně klienta a uživatelská procedura před připojením mohou před odesláním správci front provést změny v MQCONN.

Varování: V některých případech se heslo ve struktuře MQCSP pro klientskou aplikaci odešle přes síť jako prostý text. Chcete-li zajistit, aby hesla klienta aplikace byla chráněna správně, prohlédněte si téma “Ochrana heslem MQCSP” na stránce 29.

Použitím řetězce XAOPEN k zadání ID uživatele a hesla se můžete vyhnout tomu, abyste se museli měnit v kódu aplikace.

Poznámka:

V produktu IBM WebSphere MQ 6.0má uživatelská procedura zabezpečení povoleno nastavení MQCSP. Proto klienti na této úrovni nebo později nemusí být upgradováni.

Ve verzích produktu IBM MQ starších než IBM MQ 8.0však MQCSP neklade žádná omezení na ID uživatele a heslo, které aplikace poskytla. Při použití těchto hodnot s funkcemi poskytnutými produktem IBM MQ existují limity, které se vztahují na použití těchto funkcí, ale pokud je předáváte pouze svým vlastním východům, tyto limity se nepoužijí.

Související pojmy

“Ověření připojení” na stránce 66

“Ověření připojení: Konfigurace” na stránce 67

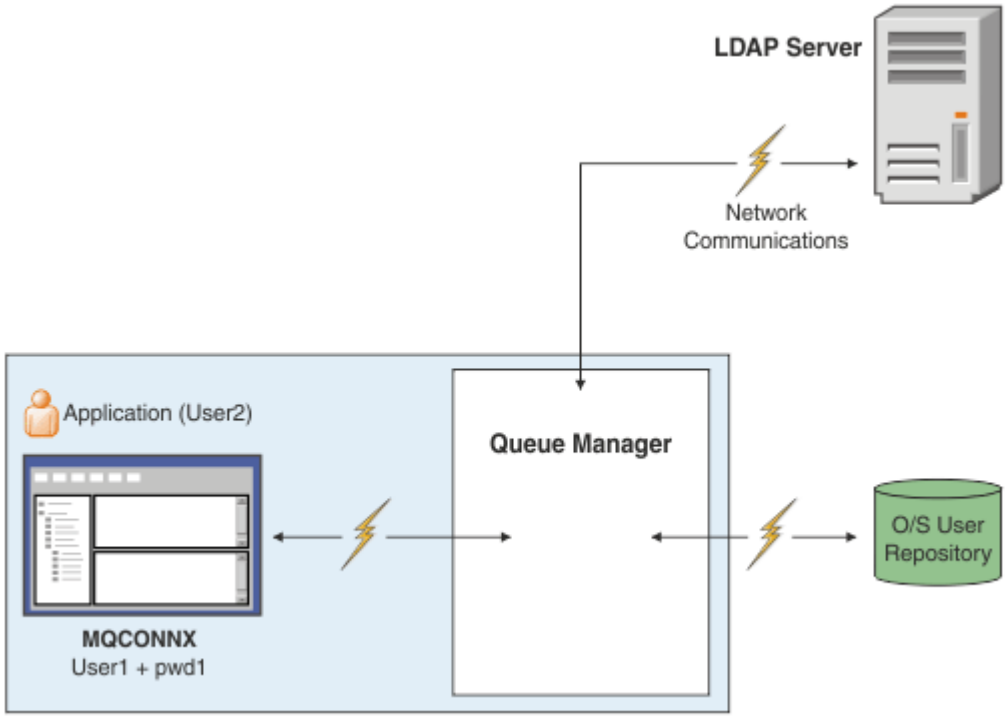
Správce front lze konfigurovat tak, aby používal zadané ID uživatele a heslo ke kontrole, zda má uživatel oprávnění pro přístup k prostředkům.

“Ověření připojení: Úložiště uživatelů” na stránce 72

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 .

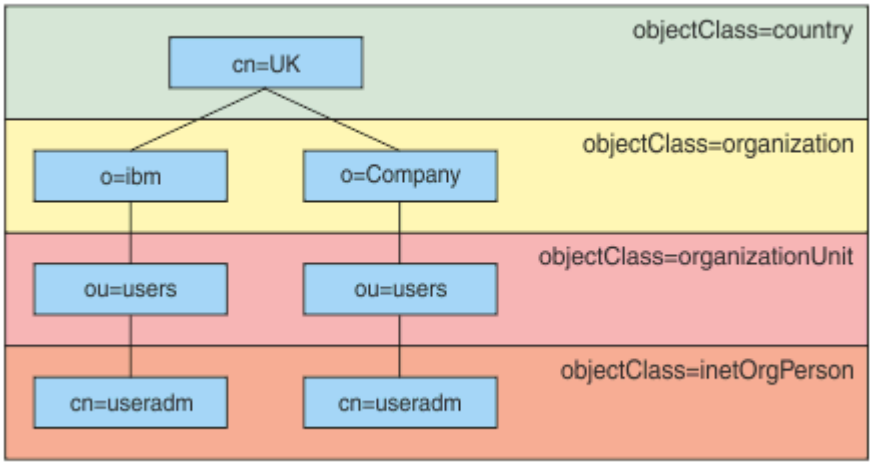
Úložiště uživatelů LDAP

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 73 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 66

“Ověření připojení: Konfigurace” na stránce 67

Správce front lze konfigurovat tak, aby používal zadané ID uživatele a heslo ke kontrole, zda má uživatel oprávnění pro přístup k prostředkům.

“Ověření připojení: Změny aplikace” na stránce 71

Uživatelská procedura zabezpečení na straně klienta pro vložení ID uživatele a hesla (`mqccred`)

Máte-li nějaké klientské aplikace, které jsou vyžadovány pro odeslání ID uživatele nebo hesla, ale nemůžete změnit zdroj, existuje uživatelská procedura zabezpečení dodávaná s produktem IBM MQ 8.0 s názvem **`mqccred`** , který můžete použít. **`mqccred`** poskytuje jménem klientské aplikace ID uživatele a heslo ze souboru `.ini` . Toto ID uživatele a heslo se odešle správci front, který, je-li nakonfigurován tak, bude ověření autentizovat.

Přehled

`mqccred` je uživatelská procedura zabezpečení, která se spouští na stejném počítači jako vaše klientská aplikace. Umožňuje zadat informace o ID uživatele a heslu pro aplikaci klienta, kde tyto informace není dodáváno samotnou aplikací. Informace o ID uživatele a heslu jsou dodány ve struktuře známé jako Parametry zabezpečení připojení (MQCSP) a budou ověřovány správcem front, pokud je konfigurováno ověřování připojení .

Informace o ID uživatele a hesle se načtou ze souboru `.ini` na klientském počítači. Hesla v souboru jsou chráněna zamaskováním pomocí příkazu **`runmqccred`** a také zajištěním oprávnění k souboru na souboru `.ini` je nastaveno tak, aby bylo možné číst pouze ID uživatele, který spouští aplikaci klienta (a tedy i ukončení).

Umístění

`mqccred` je nainstalován:

Windows platformy
V adresáři *`installation_directory`*`\Tools\c\Samples\mqccred\`

AIX and Linux platformy
V adresáři *`installation_directory`*`/samp/mqccred`

Notes: Výjezd:

1. Jedná se čistě o uživatelskou proceduru kanálu zabezpečení a potřebuje být jedinou takovou uživatelskou procedurou definovanou v kanálu.
2. Je obvykle pojmenována prostřednictvím tabulky CCDT (Client Channel Definition Table), ale klient produktu Java může mít uživatelskou proceduru uvedenou v objektech rozhraní JNDI přímo, nebo může být tato uživatelská procedura konfigurována pro aplikace, které ručně vytvoří strukturu MQCD .
3. Je třeba zkopírovat programy **`mqccred`** a **`mqccred_r`** do adresáře `var/mqm/exits` .

   Například u 64bitového 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. Je schopen pracovat na předchozích verzích produktu IBM MQ, pokud jde o IBM WebSphere MQ 7.0.1.

Nastavení ID uživatele a hesel

Soubor `.ini` obsahuje oddíly pro každého správce front, s globálním nastavením pro nespecifikované správce front. Každá stanza obsahuje jméno správce front, ID uživatele a buď prostý text, nebo zamlžené heslo.

Musíte upravit soubor `.ini` ručně, pomocí toho, který editor chcete, a přidejte atribut hesla prostého textu do oddílů. Spusťte poskytnutý, **runmqccred** program, který vezme soubor `.ini` a nahradí atribut **Password** atributem **OPW** , zamlžená formou hesla.

Popis příkazu a jeho parametrů viz runmqccred .

Soubor `mqccred.ini` obsahuje vaše ID uživatele a heslo.

Soubor šablony `.ini` se nachází ve stejném adresáři jako výstupní bod, který poskytuje výchozí bod pro váš podnik.

Při výchozím nastavení bude tento soubor vyhledán v produktu `$HOME/.mqs/mqccred.ini`. Chcete-li jej vyhledat jinde, můžete použít proměnnou prostředí *MQCCRED* tak, aby ukazovala na následující:

```
MQCCRED=C:\mydir\mqccred.ini
```

Pokud používáte *MQCCRED*, musí proměnná obsahovat úplný název konfiguračního souboru včetně všech typů souborů `.ini` . Vzhledem k tomu, že tento soubor obsahuje hesla (i když je zmatená), měli byste soubor chránit pomocí oprávnění operačního systému, aby bylo zajištěno, že jej neautorizovaní uživatelé nemohou číst. Pokud nemáte správné oprávnění k souboru, uživatelská procedura nebude úspěšně spuštěna.

Pokud aplikace již dodávala strukturu MQCSP , ukončí se uživatelská procedura standardně a nebude vkládat žádné informace ze souboru `.ini` . Toto však můžete potlačit použitím atributu **Force** v sekci.

Nastavení hodnoty **Force** na hodnotu *TRUE* odebere ID uživatele a heslo dodané aplikací a nahradí soubory s verzí ini souboru.

Chcete-li nastavit výchozí hodnotu tohoto souboru, můžete také nastavit atribut **Force** v globální sekci souboru.

Výchozí hodnota pro **Force** je *FALSE*.

Pro všechny správce front nebo pro každého jednotlivého správce front můžete zadat ID uživatele a heslo. 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. Jednotlivé definice správců front mají přednost před globálním nastavením.
2. Atributy nerozlišují velikost písmen.

Omezení

Když se tato uživatelská procedura používá, ID lokálního uživatele osoby, na které je aplikace spuštěna, nepoteče z klienta na server. Jediná dostupná informace o identitě je z obsahu ini souboru.

Proto je třeba správce front nakonfigurovat tak, aby používal produkt **ADOPTCTX(YES)**, nebo namapovat požadavek na příchozí připojení na příslušné ID uživatele prostřednictvím jednoho z dostupných mechanismů, například “Záznamy ověření kanálu” na stránce 47.

Důležité: Pokud přidáte nová hesla nebo aktualizujete staré, příkaz **runmqccred** zpracuje pouze všechna hesla prostého textu a ponechá vaše zamlžené, nedotčené.

Ladění

Výstup zapisuje do standardního trasování produktu IBM MQ , je-li tato volba povolena.

Chcete-li pomoci při ladění problémů s konfigurací, výstup může také zapisovat přímo na standardní výstup.

Žádná data uživatelské procedury zabezpečení kanálu (**SCYDATA**) je pro kanál obvykle povinná. Můžete však zadat:

CHYBA
Pouze chybové informace o chybě tisku jsou takové, jako by nebyly schopny najít konfigurační soubor.

LADĚNÍ
Zobrazí tyto chybové stavy a některé další trasovací příkazy.

NEKONTROLY
Vynechá omezení pro oprávnění k souboru a dále 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 jsou citlivé na velikost písmen a musí být zadány velkými písmeny.

Použití produktu `mqccred`

Po nastavení vašeho souboru můžete volat uživatelskou proceduru aktualizací své definice 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 spojení s klientem Java

Ověření připojení je funkce v produktu IBM MQ , která umožňuje konfigurovat správce front tak, aby mohl správce front ověřovat aplikace pomocí poskytnutého ID uživatele a hesla. Je-li aplikací aplikací produktu Java , která používá přenos klienta, může být ověření připojení spuštěno v režimu kompatibility nebo v režimu ověření MQCSP.

ID uživatele a heslo, které mají být ověřeny, je určeno aplikací pomocí jedné z následujících metod:

- V aplikaci IBM MQ classes for Java , ve třídě `MQEnvironment` nebo v tabulce vlastností Hashtable, která se předává konstruktoru `com.ibm.mq.MQQueueManager`.

- V aplikaci IBM MQ classes for JMS jako argumenty pro metodu `createConnection(String username, String Password)` nebo `createContext(String username, String password)` .

Režim ověření MQCSP

V tomto režimu je ID uživatele na straně klienta, pod kterým je spuštěna aplikace, odesláno do správce front, stejně jako ID uživatele a heslo, které mají být ověřeny. IBM MQ classes for Java a IBM MQ classes for JMS odesílají ID uživatele a heslo, které mají být ověřeny pro správce front ve struktuře MQCSP .

ID uživatele a heslo jsou k dispozici pro uživatelskou proceduru zabezpečení připojení k serveru ve struktuře MQCSP. Adresu struktury MQCSP lze najít v poli **SecurityParms** struktury MQCXP pro kanál.

Režim ověření MQCSP má následující výhody:

- Maximální délka ID uživatele, která má být ověřena, je 1024 znaků.
- Maximální délka hesla pro ověření je 256 znaků.
- Kontroly autorizace pro přístup k použití prostředků produktu IBM MQ lze provádět pomocí ID uživatele na straně klienta, pod kterým je aplikace spuštěna, když je objekt ověřovacích informací, který se používá k řízení ověření připojení na správci front, konfigurován pomocí příkazu ADOPTCTX (NO).

Režim kompatibility

Před produktem IBM MQ 8.0může klient produktu Java odeslat prostřednictvím kanálu připojení serveru ID uživatele a heslo prostřednictvím kanálu připojení klienta do kanálu připojení serveru a nechat je v polích **RemoteUserIdentifier** a **RemotePassword** struktury MQCD k dispozici pro ukončení zabezpečení. V režimu kompatibility je toto chování zachováno.

Tento režim můžete použít v kombinaci s ověřením připojení a migrovat z jakýchkoli uživatelských procedur zabezpečení, které byly dříve použity pro 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 zkráceny na 12 znaků. To může vést k selhání připojení, kód příčiny MQRC_NOT_AUTHORIZED.
- ID uživatele na straně klienta, pod kterým je aplikace spuštěna, se neodesílá správci front. Musíte buď nastavit parametr ADOPTCTX (YES) na objektu ověřovacích informací, který se používá k řízení ověření připojení ve správci front, nebo použít jinou metodu, jako je například pravidlo ověření kanálu založené na certifikátu TLS, pro nastavení ID uživatele MCA kanálu, který je kontrolován pro autorizaci pro použití prostředků produktu IBM MQ .

Výchozí režim ověření

Výchozí režim ověření, který používá aplikace klienta 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 9.2.1 Je-li v produktu IBM MQ 9.2.1zadáno jméno uživatele a heslo, je při výchozím nastavení použito ověření MQCSP.
- Pokud je zadáno ID uživatele a heslo ve verzích starších než IBM MQ 9.2.1, výchozí režim je následující:
  - Ověření MQCSP je standardně používáno aplikacemi, které používají produkt IBM MQ classes for Java.
  - Režim kompatibility je standardně používán aplikacemi, které používají produkt IBM MQ classes for JMS.
- Je-li zadáno ID uživatele, ale není zadáno žádné heslo, je při výchozím nastavení použit režim kompatibility.
- Není-li určeno žádné ID uživatele, je vždy použit režim kompatibility.

V případech, kdy je určeno ID uživatele, může aplikace pro každé jednotlivé připojení zvolit specifický režim ověření, nebo nastavit globálně před spuštěním aplikace, jak je popsáno v tématu “Volba režimu ověření” na stránce 78.

Poznámka: V 9.2.1 Aplikace, které používají produkt IBM MQ classes for JMS , mohou být ovlivněny změnou výchozího režimu ověření v produktu IBM MQ 9.2.1. Po upgradu produktu IBM MQ classes for JMS na produkt IBM MQ 9.2.1budou místo toho použity aplikace, které dříve používaly režim kompatibility při výchozím nastavení, ověření MQCSP. To může vést k tomu, že aplikace, které se dříve úspěšně připojily ke správci front, se nepřipojily k `JMSException` s kódem příčiny 2035 (MQRC_NOT_AUTHORIZED). Pokud k tomu dojde, použijte jednu z metod popsaných v “Volba režimu ověření” na stránce 78 , abyste určili, že aplikace používá režim kompatibility.

Aplikace produktu Java , které se připojují ke správci front s použitím lokálních vazeb, vždy používají režim ověřování MQCSP.

Volba režimu ověření

Režim ověření, který používají klientské aplikace produktu Java , které určují jméno uživatele při připojování ke správci front, lze určit pomocí jedné z následujících metod. Tyto metody jsou vypsány v sestupném pořadí podle priority. Není-li režim ověření určen některou z těchto metod, bude použit výchozí režim ověření.

Poznámka: V 9.2.1 Použití těchto metod pro výběr režimu ověření bylo objasněno v IBM MQ 9.2.1. V některých případech se může režim ověřování používaný klientskou aplikací produktu Java změnit, pokud je IBM MQ classes for Java nebo IBM MQ classes for JMS upgradováno na IBM MQ 9.2.1. To může vést k tomu, že aplikace, které se dříve úspěšně připojily ke správci front, se nepřipojily k `JMSException` s kódem příčiny 2035 (MQRC_NOT_AUTHORIZED). Pokud k tomu dojde, použijte jednu z následujících metod k výběru požadovaného režimu ověření.

- Určete režim ověření pro každé jednotlivé připojení nastavením příslušné vlastnosti v aplikaci před připojením ke správci front.
  - Při použití IBM MQ classes for Javanastavte vlastnost *MQConstants.USE_MQCSP_AUTHENTICATION_PROPERTY* v tabulce Hashtable, která se předává konstruktoru `com.ibm.mq.MQQueueManager` .
  - Když používáte IBM MQ classes for JMS, nastavte vlastnost *JmsConstants.USER_AUTHENTICATION_MQCSP* na příslušné faktorii připojení před vytvořením připojení.

  Nastavte hodnotu těchto vlastností na jednu z následujících hodnot:

  ano
  Při ověřování u správce front použít režim ověřování MQCSP.

  ne
  Při ověřování u správce front použijte režim kompatibility.
- Určete režim ověřování pro všechna připojení klienta, která aplikace provede, nastavením systémové vlastnosti *com.ibm.mq.cfg.jmqi.useMQCSPauthentication* Java při spouštění aplikace. Nastavte hodnotu vlastnosti na jednu z následujících hodnot:

  Y
  Při ověřování u správce front použít režim ověřování MQCSP.

  N
  Při ověřování u správce front použijte režim kompatibility.

  Následující příkaz například nastavuje vlastnost pro výběr režimu kompatibility a spouští aplikaci Java :

  ```
  java -Dcom.ibm.mq.cfg.jmqi.useMQCSPauthentication=N application_name
  ```
- Určete režim ověřování pro všechna klientská připojení aplikací spouštěná ve stejném prostředí nastavením proměnné prostředí *com.ibm.mq.jmqi.useMQCSPauthentication* v prostředí, ve kterém je aplikace spuštěna. Nastavte hodnotu proměnné prostředí na jednu z následujících hodnot:

Y
Při ověřování u správce front použít režim ověřování MQCSP.

N
Při ověřování u správce front použijte režim kompatibility.

- Určete režim ověřování pro všechny aplikace, které používají specifický konfigurační soubor klienta IBM MQ MQI client , zadáním atributu **useMQCSPauthentication** ve stanze JMQI konfiguračního souboru klienta. Nastavte hodnotu atributu na jednu z následujících hodnot:

  YES
  Při ověřování u správce front použít režim ověřování MQCSP.

  NO
  Při ověřování u správce front použijte režim kompatibility.

  Další informace o atributu **useMQCSPauthentication** naleznete v tématu Sekce JMQI konfiguračního souboru klienta.

Výběr režimu ověření v produktu IBM MQ Explorer

IBM MQ Explorer je aplikace Java , takže k němu lze použít i tyto dva režimy, režim kompatibility a režim ověření MQCSP.

V produktu IBM MQ 9.1.0je výchozím nastavením režim ověřování MQCSP. Před IBM MQ 9.1je režim kompatibility výchozí.

Na panelech, kde je poskytnuta identifikace uživatele, je zde zaškrtávací políčko pro povolení nebo zakázání režimu kompatibility:

- Z produktu IBM MQ 9.1.0toto zaškrtávací políčko standardně není zaškrtnuto. Chcete-li použít režim kompatibility, označte toto zaškrtávací políčko.
- Před IBM MQ 9.1.0je standardně toto zaškrtávací políčko povoleno. Chcete-li použít ověření MQCSP, zrušte zaškrtnutí zaškrtávacího políčka.

Související pojmy

“Ověření připojení” na stránce 66

“Ověření připojení: Změny aplikace” na stránce 71

“Ověření připojení: Úložiště uživatelů” na stránce 72
Pro každého z vašich správců front můžete zvolit různé typy objektů ověřovacích informací pro ověřování ID uživatelů a hesel.

Zabezpečení zpráv v produktu IBM MQ

Zabezpečení zpráv v infrastruktuře produktu IBM MQ poskytuje produkt Advanced Message Security.

Advanced Message Security (AMS) rozbalí služby zabezpečení produktu IBM MQ , aby poskytovaly data pro podepisování a šifrování dat na úrovni zpráv. Rozbalená služba zaručuje, že data zprávy nebyla upravena mezi okamžikem, kdy byla původně vložena do fronty, a když je načtena. Kromě toho produkt AMS ověřuje, zda je odesilatel dat zpráv autorizován k vložení podepsaných zpráv do cílové fronty.

Související pojmy

“Advanced Message Security” na stránce 581
Advanced Message Security (AMS) je komponenta produktu IBM MQ , která poskytuje vysokou úroveň ochrany citlivých dat procházejících přes síť IBM MQ , a to bez dopadu na koncové aplikace.

Plánování bezpečnostních požadavků

Tato kolekce témat vysvětluje, co je třeba zvážit při plánování zabezpečení v prostředí produktu IBM MQ .

Produkt IBM MQ lze použít pro širokou škálu aplikací na různých platformách. Požadavky na zabezpečení se pravděpodobně pro každou aplikaci liší. Pro některé bude důležitým hlediskem bezpečnost.

Produkt IBM MQ poskytuje řadu služeb zabezpečení na úrovni odkazu, včetně podpory zabezpečení TLS (Transport Layer Security).

Při plánování instalace produktu IBM MQje třeba vzít v úvahu určité aspekty zabezpečení:

- Multi Pokud v produktu Multiplatformsignorujete tyto aspekty a nedělejte nic, nemůžete použít produkt IBM MQ.
- z/OS V systému z/OSje výsledkem ignorování těchto aspektů to, že vaše prostředky IBM MQ jsou nechráněné. To znamená, že všichni uživatelé mohou přistupovat ke všem prostředkům produktu IBM MQ a měnit je.

Oprávnění ke správě produktu IBM MQ

Administrátoři produktu IBM MQ potřebují oprávnění k:

- Vydat příkazy pro správu produktu IBM MQ
- PoužijteIBM MQ Explorer
- IBM i Použijte administrativní panely a příkazy produktu IBM i .
- z/OS Použití operací a ovládacích panelů v systému z/OS
- z/OS Použijte obslužný program IBM MQ , CSQUTIL, na z/OS
- z/OS Přístup k datovým sadám správce front v systému z/OS

Další informace naleznete v následujících tématech:

- ALW “Oprávnění ke správě produktu IBM MQ v systému AIX, Linux, and Windows” na stránce 391
- IBM i “Oprávnění ke správě produktu IBM MQ v systému IBM i” na stránce 84
- z/OS “Oprávnění ke správě produktu IBM MQ v systému z/OS” na stránce 85

Oprávnění pro práci s objekty IBM MQ

Aplikace mohou přistupovat k následujícím objektům produktu IBM MQ zadáním 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 také k přístupu k kanálům a objektům ověřovacích informací. Tyto objekty mohou být chráněny produktem IBM MQ tak, aby ID uživatelů přidružená k aplikacím potřebují oprávnění pro přístup k nim.

Další informace viz “Autorizace pro aplikace, které mají být použity IBM MQ” na stránce 87.

Zabezpečení kanálu

ID uživatelů přidružená k agentům kanálu zpráv (MCA) potřebují oprávnění pro přístup k různým prostředkům produktu IBM MQ . Například, agent MCA musí být schopen připojit se ke správci front. Je-li odesílající agent MCA, musí být schopen otevřít přenosovou frontu pro kanál. Pokud se jedná o přijímající sběrnici MCA, musí být schopna otevřít cílové fronty. ID uživatelů asociovaná s aplikacemi, které potřebují spravovat kanály, iniciátory kanálu a listenery potřebují oprávnění k použití příslušných příkazů PCF. Většina aplikací však takový přístup nevyžaduje.

Další informace viz “Ověřování kanálu” na stránce 108.

Další pokyny

Následující aspekty zabezpečení je třeba vzít v úvahu pouze v případě, že používáte určitou funkci produktu IBM MQ nebo základní rozšíření produktu:

- “Zabezpečení klastrů správců front” na stránce 120
- “Zabezpečení pro publikování/odběr produktu IBM MQ” na stránce 120
- “Zabezpečení pro IBM MQ Internet Pass-Thru” na stránce 122

Plánování identifikace a ověření

Rozhodněte se, která ID uživatelů se mají použít, a jak a na jaké úrovně chcete použít ovladače ověření.

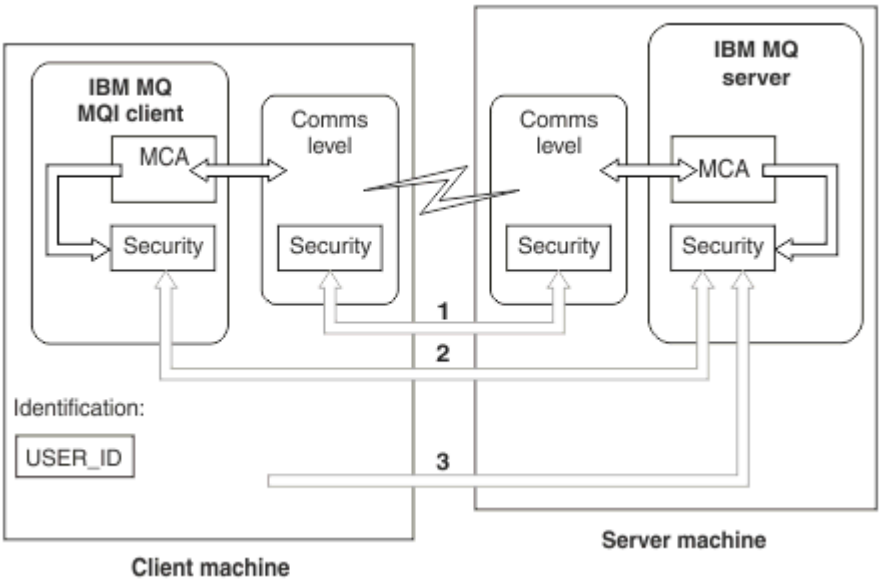
Musíte se rozhodnout, jak budete identifikovat uživatele vašich aplikací produktu IBM MQ s ohledem na to, že různé operační systémy podporují ID uživatelů různých délek. Záznamy ověření kanálu můžete použít k mapování z jednoho ID uživatele na jiný, nebo k uvedení ID uživatele na základě atributu připojení. Kanály IBM MQ používající TLS používají digitální certifikáty jako mechanismus pro identifikaci a autentizaci. Každý digitální certifikát má rozlišující název předmětu, který lze mapovat na specifické identity pomocí záznamů ověření kanálu. Certifikační certifikáty v úložišti klíčů dále určují, které digitální certifikáty lze použít k ověření produktu IBM MQ. Další informace viz:

- “Mapování vzdáleného správce front na ID uživatele MCAUSER” na stránce 376
- “Mapování ID uživatele klienta na ID uživatele MCAUSER” na stránce 377
- “Mapování rozlišovacího jména SSL nebo TLS na ID uživatele MCAUSER” na stránce 378
- “Mapování adresy IP na ID uživatele MCAUSER” na stránce 380

Plánování ověření pro klientskou aplikaci

Můžete použít ovládací prvky ověření na čtyřech úrovních: na úrovni komunikace, v bezpečnostních procedurách, se záznamy ověření kanálu a v termínech identifikace, která se předává do uživatelské procedury pro zabezpečení zprávy.

Existují čtyři úrovně zabezpečení, které je třeba vzít v úvahu. Diagram znázorňuje IBM MQ MQI client , který je připojen k serveru. Zabezpečení je použito na čtyřech úrovních, jak je popsáno v následujícím textu. MCA je agent MCA (Message Channel Agent).



Obrázek 9. Zabezpečení v připojení klient/server

1. Úroveň komunikace

   Viz šipka 1. Chcete-li implementovat zabezpečení na úrovni komunikace, použijte TLS. Další informace viz “Kryptografické bezpečnostní protokoly: TLS” na stránce 14

2. Záznamy ověření kanálu

   Viz šipky 2 & 3. Ověřování lze řídit pomocí adres IP nebo rozlišujících názvů TLS na úrovni zabezpečení. ID uživatele může být také blokováno nebo lze nasaditou ID uživatele namapovat na platné ID uživatele. Úplný popis je uveden v tématu “Záznamy ověření kanálu” na stránce 47.

3. Ověření připojení

   Viz šipka 3. Klient odešle ID a heslo. Další informace viz “Ověření připojení: Konfigurace” na stránce 67.

4. Uživatelské procedury zabezpečení kanálu

   Viz šipka 2. Ukončení zabezpečení kanálu pro komunikaci mezi klientem a serverem může fungovat stejným způsobem jako u komunikace mezi servery a serverem. K zajištění vzájemného ověření klienta i serveru může být napsána nezávislá dvojice uživatelských procedur protokolu. Úplný popis je uveden v tématu Uživatelské programy zabezpečení kanálu.

5. Identifikace, která je předána uživatelské proceduře pro zabezpečení kanálu

   Viz šipka 3. V komunikaci mezi klientem a serverem nemusí být uživatelské procedury zabezpečení kanálu fungovat jako pár. Ukončení na straně klienta IBM MQ lze vynechat. V tomto případě je ID uživatele umístěno v deskriptoru kanálu (MQCD) a uživatelská procedura zabezpečení na straně serveru ji může v případě potřeby změnit.

   Produkt IBM MQ MQI clients také odesílá další informace usnadňující identifikaci.

   - 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 zabezpečení serveru k ustanovení identity IBM MQ MQI client.

V produktu IBM MQ 8.0můžete odesílat hesla, která jsou obsažena ve struktuře MQCSP.

Varování: V některých případech se heslo ve struktuře MQCSP pro klientskou aplikaci odešle přes síť jako prostý text. Chcete-li zajistit, aby hesla klienta aplikace byla chráněna správně, prohlédněte si téma “Ochrana heslem MQCSP” na stránce 29.

ID uživatelů

Když vytváříte ID uživatelů pro klientské aplikace, ID uživatelů nesmí být delší než maximální povolená délka. Nesmíte používat vyhrazené ID uživatelů UNKNOWN a NOBODY. Pokud se server, ke kterému se klient připojuje, jedná o server IBM MQ for Windows , musíte použít znak zavináč (@). Povolená délka ID uživatele závisí na platformě, která se používá pro server:

- z/OS Linux AIX Na z/OS, AIX and Linux, maximální délka ID uživatele je 12 znaků.
- IBM i V systému IBM ije maximální délka ID uživatele 10 znaků.
- Windows Je-li v systému Windowsserver IBM MQ MQI client i server IBM MQ na serveru Windowsa server má přístup k doméně, na které je definováno ID uživatele klienta, maximální délka ID uživatele je 20 znaků. Pokud však server IBM MQ není server Windows , je ID uživatele oříznuto na 12 znaků.
- Pokud k předávání pověření používáte strukturu MQCSP, maximální délka ID uživatele je 1024 znaků. ID uživatele struktury MQCSP nelze použít k obejití maximální délky ID uživatele používaného produktem IBM MQ pro autorizaci. Další informace o struktuře MQCSP viz “Identifikace a ověřování uživatelů pomocí struktury MQCSP” na stránce 327.

Na systémech AIX and Linux se standardně používají ID uživatelů k ověření a skupiny se používají pro autorizaci. Tyto systémy však můžete nakonfigurovat tak, aby bylo možné autorizovat k ID uživatelů. Další

informace viz téma “Oprávnění pro uživatele OAM v systému AIX and Linux” na stránce 343. Systémy Windows mohou používat jak ID uživatele pro ověření, tak i autorizaci a skupiny pro autorizaci.

Pokud vytvoříte servisní účty bez nutnosti věnovat pozornost skupinám a autorizovat všechna ID uživatelů různým způsobem, může každý uživatel přistupovat k informacím o všech ostatních uživatelích.

Omezená ID uživatelů

ID uživatele UNKNOWN a skupina NOBODY mají speciální význam pro IBM MQ. Vytvoření ID uživatele v operačním systému s názvem UNKNOWN nebo skupiny s názvem NOBODY by mohlo mít nechtěné výsledky.

ID uživatelů při připojování k serveru IBM MQ for Windows

Windows

Server IBM MQ for Windows nepodporuje připojení serveru IBM MQ MQI client , pokud klient běží pod ID uživatele, které obsahuje znak @, například `abc@d`. Návratový kód pro volání `MQCONN` na klientovi je MQRC_NOT_AUTHORIZED.

Můžete však zadat jméno uživatele pomocí dvou znaků @, například `abc@@d`. Použití formátu `id@domain` je preferovanou praxí, aby bylo zajištěno, že ID uživatele je konzistentně interpretováno ve správné doméně, a tím `abc@@d@domain`.

Plánování autorizace

Naplánujte uživatele, kteří budou mít administrativní oprávnění a jak autorizovat uživatele aplikací tak, aby vhodně používali objekty produktu IBM MQ , včetně těch, které se připojují z produktu IBM MQ MQI client.

Jedincům nebo aplikacím musí být udělen přístup, aby bylo možné používat produkt IBM MQ. To, jaký přístup vyžadují, závisí na rolích, které provádějí, a na úlohách, které potřebují provést. Autorizace v produktu IBM MQ může být rozdělena do dvou hlavních kategorií:

- Oprávnění k provádění administrativních operací
- Autorizace pro aplikace, které mají být použity IBM MQ

Obě třídy operací jsou řízeny stejnou komponentou a jedinec může mít uděleno oprávnění k provedení obou kategorií operací.

Následující témata poskytují další informace o specifických oblastech autorizace, které musíte zvážit:

Oprávnění ke správě produktu IBM MQ

Administrátoři produktu IBM MQ potřebují oprávnění k provádění různých funkcí. Toto oprávnění se získá různými způsoby na různých platformách.

Administrátoři produktu IBM MQ potřebují oprávnění k:

- Zadejte příkazy pro administraci produktu IBM MQ.
- Windows Linux Použijte IBM MQ Explorer.
- z/OS Použijte operace a ovládací panely na serveru z/OS.
- z/OS Použijte obslužný program IBM MQ , CSQUTIL, na z/OS.
- z/OS Vstupte do datových sad správce front v produktu z/OS.

Další informace naleznete v tématu, které odpovídá vašemu operačnímu systému.

ALW *Oprávnění k administraci produktu IBM MQ v systémech AIX, Linux, and Windows*

Administrátor produktu IBM MQ je členem skupiny mqm. Tato skupina má přístup ke všem prostředkům IBM MQ a může vydávat řídicí příkazy IBM MQ . Administrátor může udělit určitá oprávnění jiným uživatelům.

To be an IBM MQ administrator on AIX, Linux, and Windows systems, a user must be a member of the *skupina mqm*. Tato skupina se vytvoří automaticky při instalaci produktu IBM MQ. Chcete-li uživatelům povolit, aby mohli vydávat příkazy pro řízení, musíte je přidat do skupiny mqm. To zahrnuje uživatele root na serveru AIX and Linux.

Uživatelé, kteří nejsou členy skupiny mqm, mohou mít udělena oprávnění k administraci, ale nemohou vydávat řídicí příkazy IBM MQ a mají oprávnění provádět pouze příkazy, ke kterým jim byl udělen přístup.

Kromě toho v systémech Windows mají účty SYSTEM a Administrátor úplný přístup k prostředkům produktu IBM MQ .

Všichni členové skupiny mqm mají přístup ke všem prostředkům produktu IBM MQ v systému, včetně možnosti správy libovolného správce front spuštěného v systému. Tento přístup lze odebrat pouze odebráním uživatele ze skupiny mqm. Na systémech Windows mají členové skupiny Administrátoři také přístup ke všem prostředkům produktu IBM MQ .

Administrátoři mohou použít řídicí příkaz **runmqsc** k vydání příkazu IBM MQ Script (MQSC). Je-li příkaz **runmqsc** použit v nepřímém režimu k odeslání příkazů MQSC do vzdáleného správce front, je každý příkaz MQSC zapouzdřen v rámci příkazu Escape PCF. Administrátoři musí mít požadovaná oprávnění pro příkazy MQSC, které mají být zpracovány vzdáleným správcem front.

Produkt IBM MQ Explorer vydává příkazy PCF pro provádění administrativních úloh. Administrátoři nepotřebují další oprávnění k používání produktu IBM MQ Explorer k administraci správce front v lokálním systému. Je-li produkt IBM MQ Explorer použit ke správě správce front v jiném systému, musí mít administrátoři oprávnění pro příkazy PCF, které má zpracovat vzdálený správce front.

Další informace o kontrolách oprávnění prováděných při zpracování příkazů PCF a MQSC naleznete v následujících tématech:

- Pro příkazy, které pracují se správci front, frontami, kanály, procesy, seznamy názvů a ověřovacími informacemi, viz “Autorizace pro aplikace, které mají být použity IBM MQ” na stránce 87.
- Pro příkazy, které pracují s kanály, inicializátory kanálu, listenery a klastry, naleznete informace v tématu Zabezpečení kanálů.
- z/OS Pro příkazy MQSC, které jsou zpracovány příkazovým serverem v systému IBM MQ for z/OS, viz téma “Zabezpečení příkazů a zabezpečení prostředků příkazů na systému z/OS” na stránce 86.

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 produktu IBM MQ v systému IBM i*

Chcete-li být administrátorem produktu IBM MQ na systému IBM i, musíte být členem skupiny *QMQMADM*. Tato skupina má vlastnosti podobné vlastnostem skupiny mqm na systémech AIX, Linux, and Windows . Konkrétně, skupina QMQMADM se vytvoří, když instalujete produkt IBM MQ for IBM i, a členové skupiny QMQMADM mají přístup ke všem prostředkům IBM MQ v systému. Máte-li oprávnění *ALLOBJ, máte také přístup ke všem prostředkům produktu IBM MQ .

Administrátoři mohou použít CL příkazy ke správě IBM MQ.Jedním z těchto příkazů je GRTMQMAUT, který se používá k udělování oprávnění jiným uživatelům. Jiný příkaz STRMQMMQSC umožňuje administrátorovi zadávat příkazy MQSC lokálnímu správci front.

K dispozici jsou dvě skupiny příkazů CL poskytnuté produktem IBM MQ for IBM i:

Skupina 1
Chcete-li vydat příkaz v této kategorii, uživatel musí být členem skupiny QMQMADM nebo mít oprávnění *ALLOBJ. Například GRTMQMAUT a STRMQMMQSC patří do této kategorie.

Skupina 2
Chcete-li vydat příkaz v této kategorii, uživatel nemusí být členem skupiny QMQMADM, nebo mít oprávnění *ALLOBJ. Místo toho se požadují dvě úrovně oprávnění:

- Uživatel vyžaduje oprávnění IBM i k 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 zobrazují příkazy v této skupině:

- CRTMQMQ, Vytvoření fronty MQM
- CHGMQMPRC, Změna procesu MQM
- DLTMQMNL, Výmaz seznamu názvů MQM
- DSPMQMAUTI, Zobrazení ověřovacích informací MQM
- CRTMQMCHL, Vytvoření kanálu MQM

Další informace o této skupině příkazů najdete v tématu “Autorizace pro aplikace, které mají být použity IBM MQ” na stránce 87.

Úplný seznam příkazů skupiny 1 a skupiny 2 najdete v tématu “Přístupová oprávnění pro objekty IBM MQ v systému IBM i” na stránce 153 .

Další informace o oprávnění, které potřebujete ke správě produktu IBM MQ v systému IBM i, najdete v tématu Administrace produktu IBM i .

z/OS *Oprávnění ke správě produktu 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 v systému z/OS*

IBM MQ for z/OS uses the System Authorization Facility (SAF) to route requests for authority checks to an external security manager (ESM) such as the z/OS Security Server Resource Access Control Facility (RACF). IBM MQ does no authority checks of its own.

Předpokládá se, že používáte RACF jako svůj ESM. Používáte-li jiný modul ESM, může být nutné interpretovat informace o RACF způsobem, který je pro váš ESM relevantní.

Můžete určit, zda chcete pro každého správce front jednotlivě nebo pro každého správce front ve skupině sdílení front zapnutou nebo vypnutou kontrolu oprávnění.Tato úroveň řízení se nazývá *zabezpečení subsystému*. Vypnete-li zabezpečení subsystému pro určitého správce front, nebudou pro daného správce front provedeny žádné kontroly oprávnění.

Pokud zapnete zabezpečení subsystému pro určitého správce front, mohou být kontroly oprávnění provedeny na dvou úrovních:

Zabezpečení na úrovni skupiny sdílení front
Kontroly oprávnění používají profily produktu RACF , které jsou sdíleny všemi správci front ve skupině sdílení front. To znamená, že je třeba méně profilů definovat a udržovat, což usnadňuje administraci zabezpečení.

zabezpečení na úrovni správce front
Kontroly oprávnění používají profily produktu RACF specifické pro správce front.

Můžete použít kombinaci skupiny sdílení front a zabezpečení na úrovni správce front. Můžete například zajistit, aby profily specifické pro správce front potlačují profily skupin sdílení front, do kterých 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 na systému z/OS*

Zabezpečení příkazu souvisí s oprávněním k vydání příkazu; oprávnění k prostředku příkazu se vztahuje k oprávnění k provedení operace na prostředku. Obě jsou implementovány pomocí tříd produktu RACF .

Kontroly oprávnění se provádějí, když administrátor produktu IBM MQ vydá příkaz MQSC. Tomu se říká *zabezpečení příkazu*.

Chcete-li implementovat zabezpečení příkazů, je třeba definovat určité profily produktu RACF a udělit potřebné skupiny a ID uživatelů k těmto profilům na požadovaných úrovních. Název profilu pro zabezpečení příkazů obsahuje název příkazu MQSC.

Některé příkazy MQSC provádějí operaci na prostředku IBM MQ , jako například příkaz DEFINE QLOCAL k vytvoření lokální fronty. Když administrátor vydá příkaz MQSC, provedou se kontroly oprávnění, aby se určilo, zda lze požadovanou operaci provést na prostředku uvedeném v příkazu. Tomu se říká *zabezpečení prostředků příkazů*.

Chcete-li implementovat zabezpečení na úrovni prostředků, je třeba definovat určité profily produktu RACF a udělit potřebné skupiny a ID uživatelů k těmto profilům na požadovaných úrovních. Název profilu pro zabezpečení příkazového prostředku obsahuje název prostředku IBM MQ a jeho typ (QUEUE, PROCESS, NAMELIST, TOPCIC, AUTHINFO nebo CHANNEL).

Zabezpečení příkazů a zabezpečení prostředků příkazů jsou nezávislé. Například, když administrátor vydá příkaz:

```
DEFINE QLOCAL(MOON.EUROPA)
```

jsou provedeny následující kontroly oprávnění:

- Příkaz Security Security kontroluje, že administrátor je oprávněn vydávat příkaz DEFINE QLOCAL.
- Kontrola zabezpečení prostředků příkazů kontroluje, zda je administrátor oprávněn provádět operaci s lokální frontou s názvem MOON.EUROPA.

Zabezpečení příkazů a zabezpečení prostředků příkazů lze zapnout nebo vypnout definováním profilů přepínače.

z/OS *Příkazy MQSC a vstupní fronta systémových příkazů v systému z/OS*

Toto téma vám pomůže pochopit, jak příkazový server zpracovává příkazy MQSC, které jsou směrovány do vstupní fronty systémových příkazů na systému z/OS.

Zabezpečení příkazů a zabezpečení prostředků příkazů se používají také tehdy, když příkazový server načte zprávu obsahující příkaz MQSC ze vstupní fronty příkazů systému.ID uživatele, který se použije pro kontrolu oprávnění, je ten, který se nachází v poli *UserIdentifier* v deskriptoru zprávy obsahující příkaz MQSC. Toto ID uživatele musí mít požadovaná oprávnění ve správci front, ve kterém je příkaz zpracováván. Další informace o poli *UserIdentifier* a o tom, jak je nastaveno, najdete v tématu Kontext zprávy.

Zprávy obsahující příkazy MQSC se odesílají do vstupní fronty příkazů systému za následujících okolností:

- Operace a řídicí panely odesílají příkazy MQSC do vstupní fronty příkazů systému cílového správce front. Příkazy MQSC odpovídají akcím, které jste vybrali na panelech. Pole *UserIdentifier* v každé zprávě je nastaveno na ID uživatele TSO pro administrátora.
- Funkce COMMAND obslužného programu IBM MQ , CSQUTIL, odesílá příkazy MQSC ve vstupní datové sadě do vstupní fronty příkazu systému pro 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 odeslány do vstupní fronty příkazu systému správce front, ke kterému je připojen inicializátor kanálu. Pole *UserIdentifier* v každé zprávě je nastaveno na ID uživatele adresního prostoru iniciátoru kanálu.

Když jsou příkazy MQSC vydány z datových sad CSQINP1 a CSQINP2 , žádné kontroly oprávnění se neprovedou. Můžete ovládat, kdo může aktualizovat tyto datové sady pomocí ochrany datové sady produktu RACF .

- V rámci skupiny sdílení front může inicializátor kanálu odeslat příkazy START CHANNEL do vstupní fronty příkazového řádku správce front, ke kterému je připojen. Příkaz se odešle, když se spustí odchozí kanál používající sdílenou přenosovou frontu. Pole *UserIdentifier* v každé zprávě je nastaveno na ID uživatele adresního prostoru iniciátoru kanálu.
- Aplikace může odesílat příkazy MQSC do vstupní fronty systémových příkazů. Pole *UserIdentifier* v každé zprávě je standardně nastaveno na ID uživatele přidružené k aplikaci.
- Na systémech AIX, Linux, and Windows lze řídicí příkaz **runmqsc** použít v nepřímém režimu k odesílání příkazů MQSC do vstupní fronty příkazů systému správce front v systému z/OS. Pole *UserIdentifier* v každé zprávě je nastaveno na ID uživatele administrátora, který vydal 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. Toto téma vám pomůže porozumět, které datové sady potřebují ochranu produktu RACF .

Tyto datové sady zahrnují:

- Datové sady odkazované podle CSQINP1, CSQINP2a CSQINPT v proceduře spuštěné úlohy správce front.
- Sady stránek správce front, datové sady aktivního žurnálu, datové sady protokolu archivu a zaváděcí datové sady (BSDSs).
- Datové sady odkazované podle CSQXLIB a CSQINPX v proceduře spuštěné úlohy inicializátoru kanálu

Je třeba chránit datové sady, aby žádný neautorizovaný uživatel mohl spustit správce front nebo získat přístup k datům správce front. Chcete-li to provést, použijte ochranu datové sady produktu RACF .

Autorizace pro aplikace, které mají být použity IBM MQ

Když aplikace přistupují k objektům, ID uživatelů přidružená k aplikacím potřebují odpovídající oprávnění.

Aplikace mohou přistupovat k následujícím objektům produktu IBM MQ zadáním volání MQI:

- Správci front
- Fronty
- Procesy
- Seznamy názvů
- Témata

Aplikace mohou také používat příkazy PCF ke správě objektů IBM MQ . Je-li příkaz PCF zpracován, použije kontext oprávnění ID uživatele, který vložil zprávu PCF.

Aplikace v tomto kontextu zahrnují ty, které píší uživatelé a dodavatelé, a ty, které jsou dodávané s produktem IBM MQ for z/OS. Mezi aplikace dodávané s produktem IBM MQ for z/OS patří následující:

- Ovládací panely a ovládací panely
- Obslužný program IBM MQ , CSQUTIL
- Obslužný program obslužné rutiny fronty nedoručených zpráv, CSQUDLQH

Aplikace, které používají produkt IBM MQ classes for Java, IBM MQ classes for JMS, IBM MQ classes for .NETnebo klienty Message Service Clients pro C/C++ a .NET , používají rozhraní MQI nepřímo.

MCAs také vydává volání MQI a ID uživatelů přidružená k MCAs potřebují oprávnění pro přístup k těmto objektům IBM MQ . Další informace o těchto ID uživatelů a oprávněních, která vyžadují, najdete v tématu “Ověřování kanálu” na stránce 108.

V systému z/OSmohou aplikace také používat příkazy MQSC pro přístup k těmto objektům produktu IBM MQ , ale zabezpečení příkazů a zabezpečení prostředků příkazů zajišťují oprávnění ke kontrole oprávnění

za těchto okolností. z/OS Další informace viz “Zabezpečení příkazů a zabezpečení prostředků příkazů na systému z/OS” na stránce 86 a “Příkazy MQSC a vstupní fronta systémových příkazů v systému z/OS” na stránce 86.

V systému IBM může uživatel, který vydává příkaz CL ve skupině 2, vyžadovat oprávnění pro přístup k objektu IBM MQ přidruženému k příkazu. Další informace viz “Při provádění kontrol oprávnění” na stránce 88.

Při provádění kontrol oprávnění

Kontroly oprávnění se provádějí, když se aplikace pokusí o přístup ke správci front, frontě, procesu nebo seznamu názvů.

V systému IBM imohou být kontroly oprávnění provedeny také v případě, že uživatel vydá příkaz CL ve skupině 2, který přistupuje k libovolnému z těchto objektů IBM MQ . Kontroly se provádějí za následujících okolností:

Když se aplikace připojí ke správci front pomocí volání `MQCONN` nebo `MQCONNX`

Správce front požádá operační systém o ID uživatele přidruženého k aplikaci. Správce front poté ověří, zda je ID uživatele oprávněno k jeho připojení, a zachová 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 že jsou ověřeni pomocí tohoto systému.

Když aplikace otevře objekt IBM MQ pomocí volání `MQOPEN` nebo `MQPUT1`

Všechny kontroly oprávnění se provádějí při otevření objektu, nikoli při pozdějším přístupu k objektu. Kontroly oprávnění se například provádějí, když aplikace otevře frontu. Neprovádí se, když aplikace vkládá zprávy do fronty nebo získává zprávy z fronty.

Když aplikace otevře objekt, uvádí typy operací, které je třeba provést na objektu. Například aplikace může otevřít frontu pro prohlížení zpráv na ní, získání zpráv od ní, ale ne vkládání zpráv na ni. Pro každý typ operace správce front ověří, zda má ID uživatele přidružené k aplikaci oprávnění provést tuto operaci.

Když aplikace otevře frontu, provede se kontrola oprávnění k objektu uvedenému v poli `ObjectName` v deskriptoru objektu. Pole `ObjectName` se používá na voláních `MQOPEN` nebo `MQPUT1` . Je-li objekt alias fronta nebo definice vzdálené fronty, kontroly oprávnění se provádějí proti objektu samotnému. Nejsou prováděny ve frontě, na kterou je rozlišována fronta aliasů nebo definice vzdálené fronty. To znamená, že uživatel nepotřebuje oprávnění pro přístup k němu. Omezte oprávnění k vytváření front pro privilegované uživatele. Pokud tomu tak není, uživatelé mohou obejít normální řízení přístupu pouhým 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 se provádějí proti přenosové frontě se stejným názvem jako má vzdálený správce front:

- z/OS V systému z/OSse provádí kontrola profilu fronty produktu RACF , který odpovídá názvu vzdáleného správce front, a zda je tato přenosová fronta definována lokálně, či nikoli.
- Multi V systému Multiplatformsje kontrola provedena proti profilu RQMNAME, který odpovídá názvu vzdáleného správce front, je-li používáno klastrování.

Aplikace se může odkazovat na frontu klastru explicitně nastavením pole `ObjectName` v deskriptoru objektu na název fronty klastru. Kontroly oprávnění se provádějí proti přenosové frontě klastru, `SYSTEM.CLUSTER.TRANSMIT.QUEUE`.

Oprávnění k dynamické frontě je založeno na modelové frontě, ze které je odvozena, ale nemusí být nutně stejné; viz poznámka 1.

ID uživatele, které správce front používá pro kontrolu oprávnění, je získáno z operačního systému. ID uživatele se získá, když se aplikace připojí ke správci front. Aplikace s vhodnou autorizací může vydat volání `MQOPEN` s uvedením alternativního ID uživatele; kontroly řízení přístupu se pak provedou

na alternativním ID uživatele. Použití alternativního ID uživatele nezmění ID uživatele přidružené k aplikaci, pouze ta, která se používá pro kontrolu řízení přístupu.

Když se aplikace přihlašuje k odběru tématu pomocí volání MQSUB
Když se aplikace přihlašuje k odběru tématu, určuje typ operace, kterou je třeba provést. Je to buď vytvoření odběru, změna existujícího odběru, nebo obnovení existujícího odběru, aniž by došlo ke změně. Pro každý typ operace správce front ověří, zda má ID uživatele přidružené k aplikaci oprávnění k provedení operace.

Když se aplikace přihlásí k odběru tématu, provede se kontrola oprávnění k objektům tématu, které se nacházejí ve stromu témat. Objekty tématu jsou ve stromu témat, v němž je aplikace přihlášena k odběru, ve stromu témat nebo nad nimi. Kontroly oprávnění mohou zahrnovat kontroly více než jednoho objektu tématu. ID uživatele, které správce front používá pro kontrolu oprávnění, je získáno z operačního systému. ID uživatele se získá, když se aplikace připojí ke správci front.

Správce front provádí kontroly oprávnění ve frontách odběratele, ale ne 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 , který vytvořil 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.

Je-li aplikace, která uzavře odběr, odebrána, nevytvořila ji, je nutné ji k její odebrání odebrat.

Když je příkaz PCF, který pracuje na objektu IBM MQ , zpracován příkazovým serverem
Toto pravidlo zahrnuje případ, kdy příkaz PCF pracuje s objektem ověřovacích informací.

ID uživatele, který se použije pro kontrolu oprávnění, je ten, který se nachází v poli UserIdentifier v deskriptoru zpráv příkazu PCF. Toto ID uživatele musí mít požadovaná oprávnění ve správci front, ve kterém je příkaz zpracováván. Ekvivalentní příkaz MQSC zapouzdřený v rámci příkazu Escape PCF je zpracovřen stejným způsobem. Další informace o poli UserIdentifier a o tom, jak je nastaveno, viz “kontext zprávy” na stránce 90.

IBM i **V systému IBM i, když uživatel vydává příkaz CL ve skupině 2, který pracuje na objektu IBM MQ**
Toto pravidlo zahrnuje případ, kdy příkaz CL ve skupině 2 pracuje na objektu ověřovacích informací.

Provádějí se kontroly k určení, zda má uživatel oprávnění pro práci s objektem IBM MQ přidruženým k příkazu. Kontroly se provádějí, pokud uživatel není členem skupiny QMQMADM nebo nemá oprávnění *ALLOBJ . Požadované oprávnění závisí na typu operace, kterou příkaz provádí na objektu. Například příkaz **CHGMQMQ**, Změna fronty MQM, vyžaduje oprávnění ke změně atributů fronty určené příkazem. Naproti tomu příkaz **DSPMQMQ**, který zobrazuje frontu MQM, vyžaduje oprávnění k zobrazení atributů fronty určené příkazem.

Mnoho příkazů funguje na více než jednom objektu. Chcete-li například zadat příkaz **DLTMQMQ**, odstraňte frontu MQM, jsou nezbytná následující oprávnění:

- Oprávnění pro připojení ke správci front určenému příkazem
- Oprávnění k výmazu fronty zadané příkazem

Některé příkazy pracují vůbec s žádným objektem. V tomto případě vyžaduje uživatel pouze oprávnění IBM i k vydání jednoho z těchto příkazů. **STRMQMLSR**, Spusťte modul listener MQM, je příkladem takového příkazu.

Oprávnění alternativního uživatele

Když aplikace otevře objekt nebo se přihlásí k odběru tématu, může aplikace dodat ID uživatele v rámci volání MQOPEN, MQPUT1nebo MQSUB. Může požádat správce front o použití tohoto ID uživatele pro kontroly oprávnění namísto toho, který je přidružen k aplikaci.

Aplikace uspěje při otevírání objektu, pouze pokud jsou splněny obě následující podmínky:

- ID uživatele přidružené k aplikaci má oprávnění k poskytnutí jiného ID uživatele pro kontroly oprávnění. Aplikace se říká, že má mít *alternativní oprávnění uživatele*.

- ID uživatele zadané aplikací má oprávnění k otevření objektu pro požadované typy operací nebo pro přihlášení k odběru tématu.

kontext zprávy

Informace *Kontext zprávy* umožňují aplikaci, která načte zprávu, zjistit informace o odesílateli zprávy. Informace se nacházejí v polích v deskriptoru zpráv a pole jsou rozdělena do tří logických částí.

Jedná se o následující části:

kontext identity
Tato pole obsahují informace o uživateli aplikace, která vložila zprávu do fronty.

výchozí kontext
Tato pole obsahují informace o samotné aplikaci a o tom, kdy byla zpráva vložena do fronty.

kontext uživatele
Tato pole obsahují vlastnosti zpráv, které aplikace mohou použít k výběru zpráv, které by měl správce front dodat.

Když aplikace vloží zprávu do fronty, může požádat správce front, aby generoval informace o kontextu ve zprávě. Toto je výchozí akce. Alternativně může uvést, že pole kontextu nemají obsahovat žádné informace. ID uživatele přidružené k aplikaci nevyžaduje žádné speciální oprávnění, které by bylo možné provést pro jednu z těchto položek.

Aplikace může nastavit pole kontextu identity ve zprávě a umožnit správci front generovat kontext původu, nebo může nastavit všechna pole kontextu. Aplikace může také předat pole kontextu identity ze zprávy, která byla načtena do zprávy, která je umístěna do fronty, nebo může projít 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 při otevření fronty, v níž má být vložila zprávy, a v tomto okamžiku je zkontrolováno jeho oprávnění.

Zde je stručný popis každého z kontextových polí:

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, když se aplikace připojí ke správci front.

AccountingToken
Informace, které lze použít k nabití za práci provedenou jako výsledek zprávy.

ApplIdentityData
Má-li ID uživatele přidružené k aplikaci oprávnění k nastavení polí kontextu identity nebo pro nastavení všech polí kontextu, může aplikace nastavit toto pole na jakoukoli hodnotu související s identitou. Pokud toto pole nastavuje správce front, je tato pole nastavena na prázdnou hodnotu.

Původní kontext

PutApplType
Typ aplikace, která vložila tuto zprávu; například transakce CICS .

PutApplName
Název aplikace, která vložila zprávu.

PutDate
Datum, kdy byla zpráva vložena.

PutTime
Čas, kdy byla zpráva vložena.

ApplOriginData
Má-li ID uživatele přidružené k aplikaci oprávnění nastavit všechna pole kontextu, může aplikace nastavit toto pole na jakoukoli hodnotu související s původem. Pokud toto pole nastavuje správce front, je tato pole nastavena na prázdnou hodnotu.

Kontext uživatele

Následující hodnoty jsou podporovány pro **MQINQMP** nebo **MQSETMP**:

M_KONTEXT MQPD_USER

Vlastnost je přidružena ke kontextu uživatele.

K nastavení vlastnosti přidružené k kontextu uživatele pomocí volání MQSETMP není vyžadována žádná speciální autorizace.

Na serveru V7.0 nebo následujícím správci front je vlastnost přidružená k uživatelskému kontextu uložena, jak je popsáno pro MQOO_SAVE_ALL_CONTEXT. Volba MQPUT s parametrem MQOO_PASS_ALL_CONTEXT způsobí, že vlastnost bude zkopírována z uloženého kontextu do nové zprávy.

MQPD_NO_CONTEXT

Vlastnost není přidružena ke kontextu zprávy.

Nerozpoznaná hodnota byla odmítnuta s funkcí MQRC_PD_ERROR. Počáteční hodnota tohoto pole je **MQPD_NO_CONTEXT**.

Podrobný popis jednotlivých polí kontextu viz MQMD-Message descriptor. Další informace o tom, jak používat kontext zprávy, najdete v tématu Kontext zprávy.

IBM i ALW *Oprávnění pro práci s objekty IBM MQ na systémech* IBM i *IBM i , AIX, Linux, and Windows*

Komponenta autorizační služby poskytnutá s produktem IBM MQ se nazývá *správce oprávnění k objektu* (OAM). Poskytuje řízení přístupu prostřednictvím kontrol ověření a autorizace.

Ověřování.

Kontrola ověření provedená pomocí OAM dodávaná s produktem IBM MQ je základní a je prováděna pouze za určitých okolností. Nepředpokládá se, že by splňujete přísné požadavky, které se očekávají ve vysoce zabezpečeném prostředí.

OAM provádí kontrolu ověření, když se aplikace připojuje ke správci front, a následující podmínky jsou pravdivé:

- Pokud byla struktura MQCSP dodána připojovanou aplikací, a
- Atribut *AuthenticationType* ve struktuře MQCSP má hodnotu MQCSP_AUTH_USER_ID_AND_PWD a
- Hodnota CHCKLOCL nebo CHKCCLNT na konfigurovaném objektu AUTHINFO není 'NONE'

Kroky ověření v OAM validují heslo pomocí služeb operačního systému, které mohly být nakonfigurovány pro provedení dalších kontrol, jako je například zajištění, že jméno uživatele nemá příliš mnoho chybných pokusů o zadání hesla.

Je možné použít alternativní mechanismy ověření, pokud jste napsali novou komponentu autorizační služby, nebo jste obdrželi jeden od dodavatele.

Autorizace.

Kontroly autorizace jsou komplexní a jsou určeny ke splnění většiny běžných požadavků.

Kontroly autorizace jsou prováděny, když aplikace vydá volání MQI pro přístup ke správci front, frontě, procesu, tématu nebo seznamu názvů. Provádějí se také v jiných případech, například když je příkaz prováděn příkazovým serverem.

Na 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 pro alternativní oprávnění uživatele a oprávnění k nastavení nebo předání informací o kontextu.

Windows V systému Windows dává produkt OAM členům skupiny administrátorů oprávnění pro přístup ke všem objektům IBM MQ i v případě, že je povolen přístup UAC. Kromě toho má účet SYSTEM v systémech Windows úplný přístup k prostředkům produktu IBM MQ .

Autorizační služba také poskytuje oprávnění ke kontrole, když příkaz PCF pracuje na jednom z těchto objektů IBM MQ nebo na objektu ověřovacích informací. Ekvivalentní příkaz MQSC zapouzdřený v rámci příkazu Escape PCF je zpracovřen stejným způsobem.

IBM i On IBM i , unless the user is a member of the QMQMADM group or has *ALLOBJ authority, the authorization service also provides authority checks when a user issues a CL command in Group 2 that operates on any of these IBM MQ objects or an authentication information object.

Autorizační služba je *instalovatelná služba*, což znamená, že je implementována jednou nebo více *instalovatelnými komponentami služeb*. Každá komponenta je vyvolána pomocí dokumentovaného rozhraní. To umožňuje uživatelům a dodavatelům poskytovat komponenty k rozšiřování nebo nahrazování komponent poskytovaných produkty IBM MQ .

Komponenta autorizační služby poskytnutá s produktem IBM MQ se nazývá správce oprávnění k objektu (OAM). OAM je automaticky povolena pro každého vytvářený správce front.

OAM udržuje seznam přístupových práv (ACL) pro každý objekt produktu IBM MQ , ke kterému má oprávnění přístup. V systémech AIX and Linux se mohou v seznamu přístupových práv zobrazit pouze ID skupin. To znamená, že všichni členové skupiny mají stejné oprávnění. Na systémech IBM i IBM i a na Windows se mohou v seznamu ACL objevit jak ID uživatele, tak ID skupin. To znamená, že oprávnění mohou být udělována jednotlivým uživatelům a skupinám.

Pro skupinu i ID uživatele platí omezení pro 12 znaků. Platformy UNIX obecně omezují délku ID uživatele na 12 znaků. AIX a Linux zvýšily tento limit, ale produkt IBM MQ pokračuje ve sledování 12 znaků omezení na všech platformách UNIX . Použijete-li ID uživatele delší než 12 znaků, nahradí jej produkt IBM MQ hodnotou "NEZNÁMÝ". Nedefinujte ID uživatele s hodnotou "UNKNOWN".

OAM může ověřit uživatele a změnit odpovídající pole kontextu identity. Povolíte to zadáním struktury parametrů zabezpečení připojení (MQCSP) na volání MQCONNX. Struktura se předává do funkce ověření uživatele OAM Authenticate User (MQZ_AUTHENTICATE_USER), která nastavuje příslušná pole kontextu identity. Je-li připojení MQCONNX z klienta IBM MQ , informace v MQCSP se tečí do správce front, ke kterému se klient připojuje prostřednictvím kanálu připojení klienta a serveru. Jsou-li na tomto kanálu definovány uživatelské procedury zabezpečení, je MQCSP předán do každé uživatelské procedury zabezpečení a může být jejím ukončením změněn. Uživatelské procedury zabezpečení mohou také vytvořit MQCSP. Další podrobnosti o použití uživatelských procedur zabezpečení v tomto kontextu najdete v tématu Uživatelské programy zabezpečení kanálu.

Varování: V některých případech se heslo ve struktuře MQCSP pro klientskou aplikaci odešle přes síť jako prostý text. Chcete-li zajistit, aby hesla klientských aplikací byla chráněna odpovídajícím způsobem, prohlédněte si téma Ochrana heslem produktuIBM MQCSP.

V systémech AIX, Linux, and Windows příkaz řízení **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 , který je ve vlastnictví správce front JUPITER. Umožňuje členům také získávat zprávy z fronty. Chcete-li odvolat tyto oprávnění později, 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 jakékoli fronty s názvem, který začíná znaky MOON.. MOON.* je název generického profilu.*Generický profil* vám umožňuje udělit oprávnění pro sadu objektů pomocí jednoho příkazu **setmqaut** .

Řídící příkaz **dspmqaut** je k dispozici pro zobrazení aktuálních oprávnění, které má uživatel nebo skupina pro uvedený objekt.Řídicí příkaz **dmpmqaut** je také k dispozici pro zobrazení aktuálních oprávnění asociovaných s generickými profily.

IBM i Administrátor v systému IBM ipoužívá příkaz CL GRTMQMAUT k udělení oprávnění a CL příkaz RVKMQMAUT k odvolání oprávnění. Lze také použít generické profily.Například CL příkaz:

```
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 jakékoli fronty se jménem, které začíná znaky `MOON.`

IBM i Příkaz CL DSPMQMAUT zobrazuje aktuální oprávnění, která má uživatel nebo skupina pro uvedený objekt. Příkazy CL WRKMQMAUT a WRKMQMAUTD jsou také k dispozici pro práci s aktuálními oprávněními asociovanými s objekty a generickými profily.

Pokud nechcete žádné kontroly oprávnění, například v testovacím prostředí, můžete zakázat OAM.

Multi *Použití příkazu 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
Zjistit oprávnění entity	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 být prováděny uživateli v libovolné skupině, které byly uděleny příkazy dsp a chg ve správci front.

Další informace o použití těchto příkazů najdete v tématu Úvod do formátu programových příkazů.

z/OS *Oprávnění pro práci s objekty IBM MQ v systému z/OS*

V systému z/OSexistuje sedm kategorií kontroly oprávnění, které jsou přidruženy k volání MQI. Musíte definovat určité profily produktu RACF a poskytnout odpovídající přístup k těmto profilům. Pomocí profilu *RESLEVEL* můžete určit, kolik ID uživatelů bude kontrolováno.

Sedm kategorií kontrol oprávnění souvisejících s voláními do rozhraní MQI:

Zabezpečení připojení
Kontroly oprávnění, které jsou provedeny při připojování aplikace ke správci front

Zabezpečení fronty
Kontroly oprávnění, které jsou prováděny, když aplikace otevře frontu nebo odstraní trvalou dynamickou frontu

Zabezpečení procesu
Kontroly oprávnění, které jsou provedeny, když aplikace otevře objekt procesu.

Zabezpečení seznamu názvů
Kontroly oprávnění, které se provedou, když aplikace otevře objekt seznamu názvů

alternativní zabezpečení uživatele
Kontroly oprávnění, které jsou provedeny, když aplikace při otevírání objektu požaduje alternativní oprávnění uživatele

zabezpečení kontextu
Kontroly oprávnění, které jsou provedeny při otevření fronty aplikací a uvádí, že má v úmyslu nastavit nebo předat informace o kontextu ve zprávách, které vkládá do fronty.

Zabezpečení tématu
Kontroly oprávnění, které jsou provedeny při otevření tématu aplikace.

Každá kategorie kontroly oprávnění je implementována stejným způsobem, jakým je implementováno zabezpečení příkazů a zabezpečení prostředků příkazů. Musíte definovat určité profily produktu RACF a udělit potřebné skupiny a ID uživatelů k těmto profilům na požadovaných úrovních. V případě zabezpečení fronty určuje úroveň přístupu typy operací, které může aplikace provádět ve frontě. V kontextu zabezpečení kontextu úroveň přístupu určuje, zda aplikace může:

- Předat všechna pole kontextu
- Předat všechna pole kontextu a nastavit pole kontextu identity
- Předat a nastavit všechna pole kontextu

Každá kategorie kontroly oprávnění může být zapnuta nebo vypnuta definováním profilů přepínače.

Všechny kategorie, kromě zabezpečení připojení, jsou souhrnně označovány jako *zabezpečení na úrovni rozhraní API*.

Je-li v důsledku volání MQI z aplikace pomocí dávkového připojení provedena kontrola zabezpečení pomocí rozhraní API, je zkontrolováno pouze jedno ID uživatele, pokud je kontrola zabezpečení prostředku API provedena. Je-li kontrola provedena jako výsledek volání MQI z aplikace CICS nebo IMS , nebo z inicializátoru kanálu, jsou zkontrolována dvě ID uživatelů.

Definováním *profilu RESLEVEL*však můžete řídit, zda jsou zaškrtnuta nula, jedna nebo dvě ID uživatelů. Počet ID uživatelů, které jsou zkontrolovány, je určen ID uživatele přidruženého 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 připojované úlohy pro dávkové připojení
- ID uživatele adresního prostoru CICS pro připojení CICS
- ID uživatele adresního prostoru IMS pro připojení IMS
- ID uživatele adresního prostoru iniciátoru kanálu pro připojení inicializátoru kanálu

Další informace o oprávnění pro práci s objekty produktu IBM MQ v systému z/OSnaleznete v tématu “Oprávnění ke správě produktu IBM MQ v systému z/OS” na stránce 85.

Zabezpečení pro vzdálený systém zpráv

Tento oddíl pojednává o aspektech zabezpečení vzdáleného systému zpráv.

Musíte uživatelům poskytnout oprávnění k používání zařízení produktu IBM MQ . To je organizováno v závislosti na akcích, které mají být provedeny s ohledem na objekty a definice. Příklad:

- Správci front mohou být spuštění a zastaveni autorizovanými uživateli.
- Aplikace se musí připojit ke správci front a mít oprávnění k použití front.
- Kanály zpráv musí být vytvářeny a řízeny oprávněnými uživateli.
- Objekty jsou uchovány v knihovnách a přístup k těmto knihovnám může být omezen

Agent kanálu zpráv na vzdáleném serveru musí zkontrolovat, zda zpráva, která je doručena, pochází od uživatele s oprávněním, aby tak mohl učinit na tomto vzdáleném serveru. Kromě toho je možné, že jako MCAs může být spuštěno vzdáleně, může být nezbytné ověřit, zda se vzdálené procesy pokoušejí spustit vaše MCA, k tomu mají oprávnění. Existují čtyři možné způsoby, jak se s tím vypořádat:

1. Proveďte odpovídající použití atributu PutAuthority u definice kanálu RCVR, RQSTR nebo CLUSRCVR, abyste mohli řídit, který uživatel se bude používat pro kontroly autorizace v době, kdy jsou do vašich front vloženy příchozí zprávy. Viz popis příkazu DEFINE CHANNEL v příručce příkazů MQSC.

2. Chcete-li odmítnout nechtěné pokusy o připojení nebo nastavit hodnotu MCAUSER na základě následujících údajů: vzdálenou adresu IP, ID vzdáleného uživatele, zadaný rozlišující název (DN) vzdáleného uživatele nebo název vzdáleného správce front, implementujte záznamy ověření kanálu, nebo nastavte hodnotu MCAUSER na základě následujících údajů:
3. Implementujte kontrolu zabezpečení *uživatelských procedur* , abyste se ujistili, že je odpovídající kanál zpráv autorizován. Zabezpečení instalace hostujícího odpovídající kanál zajišťuje, aby všichni uživatelé byli řádně autorizováni, takže nemusíte kontrolovat jednotlivé zprávy.
4. Implementujte zpracování zpráv *uživatelské procedury* , abyste se ujistili, že jednotlivé zprávy jsou prověřeny pro autorizaci.

IBM i *Zabezpečení objektů IBM MQ for IBM i*

Tento oddíl pojednává o aspektech zabezpečení vzdáleného systému zpráv.

Musíte poskytnout uživatelům s oprávněním, aby mohli využívat zařízení produktu IBM MQ for IBM i . Toto oprávnění je organizováno v závislosti na akcích, které mají být provedeny s ohledem na objekty a definice. Příklad:

- Správci front mohou být spuštění a zastaveni autorizovanými uživateli.
- Aplikace se musí připojit ke správci front a mají oprávnění pro použití front.
- Kanály zpráv musí být vytvořeny a řízeny oprávněnými uživateli.

Agent kanálu zpráv na vzdáleném serveru musí zkontrolovat, zda je doručovaná zpráva odvozena od uživatele s oprávněním, aby zadal zprávu na tomto vzdáleném serveru. Kromě toho je možné, že jako MCAs může být spuštěno vzdáleně, může být nezbytné ověřit, zda se vzdálené procesy pokoušejí spustit vaše MCA, k tomu mají oprávnění. Existují čtyři možné způsoby, jak se s tím vypořádat:

- Vyhláška v definici kanálu, že zprávy musí obsahovat přijatelný *kontext* oprávnění, jinak budou zahozeny.
- Chcete-li odmítnout nechtěné pokusy o připojení nebo nastavit hodnotu MCAUSER na základě jedné z následujících možností: vzdálenou adresu IP, jméno vzdáleného uživatele, jméno vzdáleného uživatele a jméno vzdáleného správce front, implementujte záznamy o vzdáleném ID uživatele, ID vzdáleného uživatele, jméno vzdáleného uživatele a jméno vzdáleného správce front, které jsou uvedeny na jedné z následujících možností: vzdálená IP adresa, ID vzdáleného uživatele,
- Implementujte kontrolu zabezpečení ukončení uživatele, abyste se ujistili, že je odpovídající kanál zpráv autorizován. Zabezpečení instalace hostujícího odpovídající kanál zajišťuje, aby všichni uživatelé byli řádně autorizováni, takže nemusíte kontrolovat jednotlivé zprávy.
- Implementujte zpracování zpráv uživatelské procedury a ujistěte se, že jednotlivé zprávy jsou prověřeny pro autorizaci.

Zde je několik faktů o způsobu, jakým produkt IBM MQ for IBM i obsluhuje zabezpečení:

- Uživatelé jsou identifikováni a ověřeni produktem IBM i.
- Služby správce front vyvolané aplikacemi jsou spouštěny s oprávněním uživatelského profilu správce front, ale v rámci procesu uživatele.
- Služby správce front vyvolané příkazy uživatele jsou spuštěny s oprávněním uživatelského profilu správce front.

Linux AIX *Zabezpečení objektů v systému AIX and Linux*

Administrační uživatelé musí být součástí skupiny mqm na vašem systému (včetně uživatele root), pokud toto ID bude používat příkazy administrace produktu IBM MQ .

Vždy byste měli spouštět příkaz amqcrsta jako ID uživatele "mqm".

ID uživatelů v systému AIX and Linux

Správce front převede všechna velká nebo smíšená jména uživatelů případu na malá písmena. Správce front poté vloží identifikátory uživatelů do kontextové části zprávy nebo zkontroluje jejich autorizaci. Oprávnění jsou proto založena pouze na identifikátorech malých písmen.

Windows *Zabezpečení objektů v systémech Windows*

Administrační uživatelé musí být součástí skupiny mqm a skupiny administrátorů na systémech Windows , pokud toto ID bude používat příkazy administrace produktu IBM MQ .

ID uživatelů na systémech Windows

Pokud v systémech Windows *není-li instalována žádná uživatelská procedura pro zprávy*, bude správce front převeden na malá písmena nebo se smíšenými malými a velkými písmeny a velkými písmeny. Správce front poté vloží identifikátory uživatelů do kontextové části zprávy nebo zkontroluje jejich autorizaci. Oprávnění jsou proto založena pouze na identifikátorech malých písmen.

ID uživatelů v rámci systémů

Platformy jiných než AIX, Linux, and Windows systémů používají velká písmena pro ID uživatelů ve zprávách. Chcete-li systému AIX, Linux, and Windows umožnit používání malých uživatelských jmen ve zprávách, musí agent MCA (Message Channel Agent) provést odpovídající převody abecedních znaků.

Chcete-li umožnit systému AIX, Linux, and Windows používat malá jména uživatelů ve zprávách, provede na těchto platformách následující konverze na těchto platformách:

Na odesílající straně
Abecední znaky ve všech ID uživatelů jsou převedeny na velká písmena, pokud není nainstalována žádná uživatelská procedura pro zprávy.

Na přijímajícím konci
Abecední znaky ve všech ID uživatelů jsou převedeny na malá písmena, pokud není nainstalována žádná uživatelská procedura pro ukončení zprávy.

Automatické konverze se neprovedou, pokud poskytnete ukončení zprávy na serveru AIX, Linux, and Windows z jakékoli jiné příčiny.

Použití vlastní autorizační služby

Produkt IBM MQ poskytuje instalovatelnou autorizační službu. Můžete zvolit instalaci alternativní služby.

Komponenta autorizační služba dodaná s produktem IBM MQ se nazývá OAM (Object Authority Manager). Pokud produkt OAM neposkytuje potřebná oprávnění k autorizaci, můžete napsat vlastní komponentu autorizační služby. Instalovatelné funkce služby, které musí být implementovány komponentou autorizační služby, jsou popsány v tématu Referenční informace o rozhraní instalovatelných služeb.

Řízení přístupu pro klienty

Řízení přístupu je založeno na ID uživatelů. Pro správu může být mnoho ID uživatelů a ID uživatelů mohou být v různých formátech. Můžete nastavit vlastnost kanálu připojení serveru MCAUSER na speciální hodnotu ID uživatele, aby ji mohli používat klienti.

Řízení přístupu v produktu IBM MQ je založeno na ID uživatelů. ID uživatele procesu, který provádí volání MQI, se obvykle používá. Pro klienty MQ MQI je služba MCA pro připojení serveru znepřístupnila volání MQI pro klienty MQ MQI. Můžete vybrat alternativní ID uživatele pro produkt MCA připojení k serveru, který má být použit při vytváření volání MQI. Alternativní ID uživatele může být přidruženo buď k pracovní stanici klienta, nebo k tomu, co vyberete pro uspořádání a řízení přístupu klientů. ID uživatele musí mít k dispozici potřebná oprávnění, která jsou na serveru přidělena k vydávání volání MQI. Výběr alternativního ID uživatele je vhodnější, než umožníte klientům, aby učinili volání MQI s oprávněním agenta MCA připojení k serveru.

Tabulka 9. ID uživatele použité kanálem připojení serveru	
Jméno uživatele	**Při použití**
ID uživatele, které je nastaveno uživatelskou procedurou zabezpečení	Používá se, pokud není blokováno pravidlem **CHLAUTH TYPE(BLOCKUSER)** . Další informace najdete v následující sekci “Nastavení ID uživatele v uživatelské proceduře pro zabezpečení zprávy” na stránce 97 .
ID uživatele, který je nastaven pravidlem CHLAUTH	Použije se, pokud není přepsáno uživatelskou procedurou zabezpečení. Další informace naleznete v tématu Záznamy ověřování kanálu .
ID uživatele, které je definováno v atributu **MCAUSER** v definici kanálu SVRCONN	Používá se, pokud není přepsáno uživatelskou procedurou zabezpečení nebo pravidlem CHLAUTH.
ID uživatele, které je přenášena z počítače klienta	Používá se, když žádné ID uživatele není nastaveno žádnými jinými prostředky.
ID uživatele, který spustil kanál připojení serveru	Používá se, když není žádné ID uživatele nastaveno žádnými jinými prostředky a žádné ID uživatele klienta není přenášené. Další informace najdete v následující sekci “ID uživatele, který spouští program kanálu.” na stránce 98 .

Vzhledem k tomu, že připojení MCA pro připojení k serveru provádí volání MQI pro vzdálené uživatele, je důležité vzít v úvahu bezpečnostní důsledky připojení MCA pro připojení k serveru pro vzdálené klienty a způsob správy přístupu potenciálně velkého počtu uživatelů.

- Jeden přístup je pro server MCA připojení k serveru, aby mohl volat volání MQI na vlastní oprávnění. Ale pozor, je to obvykle nežádoucí pro server MCA připojení serveru se svými výkonnými schopnostmi přístupu k odesílání volání MQI pro uživatele klienta.
- Jiný přístup spočívá v použití ID uživatele, které teče z klienta. Agent MCA připojení k serveru může volat volání MQI s využitím možností přístupu pro ID uživatele klienta. Tento přístup představuje řadu otázek, které je třeba vzít v úvahu:
  1. Pro ID uživatele na různých platformách existují různé formáty. To někdy způsobí problémy, pokud se formát ID uživatele na klientovi liší od přijatelných formátů na serveru.
  2. Existuje potenciálně mnoho klientů s různými a změna ID uživatelů. ID musí být definována a spravována na serveru.
  3. Je ID uživatele důvěryhodné? Libovolné ID uživatele může být tečeno z klienta, ne nutně ID přihlášeného uživatele. Klient může například proudit ID s úplným oprávněním `mqm` , které bylo záměrně definováno pouze na serveru z důvodů zabezpečení.
- Upřednostňovaný přístup je definovat tokeny identifikace klienta na serveru, a tak omezit schopnosti aplikací připojených ke klientovi. To se obvykle provádí nastavením vlastnosti kanálu připojení serveru MCAUSER na speciální hodnotu ID uživatele, které mají být použity klienty, a definování několika ID pro použití klienty s odlišnou úrovní autorizace na serveru.

Nastavení ID uživatele v uživatelské proceduře pro zabezpečení zprávy

Pro produkt IBM MQ MQI clientsje proces, který vydává volání MQI, serverem MCA připojení k serveru. ID uživatele použité rozhraním MCA pro připojení k serveru je obsaženo v polích `MCAUserIdentifier` nebo `LongMCAUserIdentifier` na disku MQCD. Obsah těchto polí je nastaven takto:

- Libovolné hodnoty nastavené uživatelskými procedurami pro zabezpečení
- ID uživatele z klienta
- MCAUSER (v kanálu-definice kanálu připojení)

Uživatelská procedura zabezpečení může přepsat hodnoty, které jsou pro něj viditelné, když je vyvoláno.

- Je-li atribut MCAUSER kanálu připojení serveru MCAUSER nastaven na hodnotu nonblank, je použita hodnota MCAUSER.
- Je-li atribut MCAUSER kanálu připojení serveru prázdný, použije se ID uživatele přijaté od klienta.
- Je-li atribut MCAUSER kanálu připojení serveru prázdný a od klienta není obdrženo žádné ID uživatele, použije se ID uživatele, které spustil kanál připojení serveru.

Klient produktu IBM MQ nevyužívá při použití uživatelské procedury zabezpečení na straně klienta deklarovanou ID uživatele na server.

ID uživatele, který spouští program kanálu.

Když jsou pole ID uživatele odvozena od ID uživatele, který spustil kanál připojení serveru, použije se tato hodnota:

- z/OS Pro produkt z/OSje ID uživatele přiřazeného ke spuštěné úloze iniciátoru kanálu spuštěné v tabulce procedur spuštěných z/OS .
- Pro TCP/IP (non- z/OS), ID uživatele z položky `inetd.conf` nebo ID uživatele, který spustil modul listener.
- Pro SNA (non- z/OS), ID uživatele z položky 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 definice kanálu připojení serveru, které mají nastaven atribut MCAUSER na prázdnou hodnotu, klienti mohou tuto definici kanálu použít k připojení ke správci front s oprávněním pro přístup určeným ID uživatele dodaným klientem. Může se jednat o bezpečnostní riziko, pokud systém, v němž je správce front spuštěn, umožňuje neautorizované síťové připojení. Výchozí kanál připojení serveru IBM MQ (SYSTEM.DEF.SVRCONN) má atribut MCAUSER nastaven na prázdnou hodnotu. Chcete-li zabránit neoprávněnému přístupu, aktualizujte atribut MCAUSER výchozí definice se jménem uživatele, které nemá přístup k objektům produktu IBM MQ MQ .

Velikost písmen ID uživatele

Definujete-li kanál pomocí `runmqsc`, změní se atribut MCAUSER na velká písmena, pokud se ID uživatele nevejde do jednoduchých uvozovek.

ALW U serverů v systému AIX, Linux, and Windowsse obsah pole `MCAUserIdentifier` přijatého od klienta změní na malá písmena.

IBM i U serverů v systému IBM ise obsah pole `LongMCAUserIdentifier` přijatého od klienta změní na velká písmena.

Linux AIX U serverů v systémech AIX and Linux je obsah pole `LongMCAUserIdentifier` obdržený od klienta změněn na malá písmena.

Při výchozím nastavení je ID uživatele, které je předáno při použití vazby IBM MQ JMS , ID uživatele pro prostředí JVM, na kterém je aplikace spuštěna.

ID uživatele je také možné předat pomocí metody `createQueueConnection` .

Plánování utajení

Naplánujte, jak uchovávat vaše data důvěrná.

Důvěryhodnost můžete implementovat na úrovni aplikace nebo na úrovni odkazů. Můžete se rozhodnout použít TLS, v tom případě musíte naplánovat použití digitálních certifikátů. Ukončovací programy kanálu můžete také použít, pokud standardní vybavení nevyhovují vašim požadavkům.

Související pojmy

“Porovnání zabezpečení na úrovni odkazů a zabezpečení na úrovni aplikace” na stránce 99
Toto téma obsahuje informace o různých aspektech zabezpečení na úrovni odkazů a zabezpečení na úrovni aplikací a porovnává dvě úrovně zabezpečení.

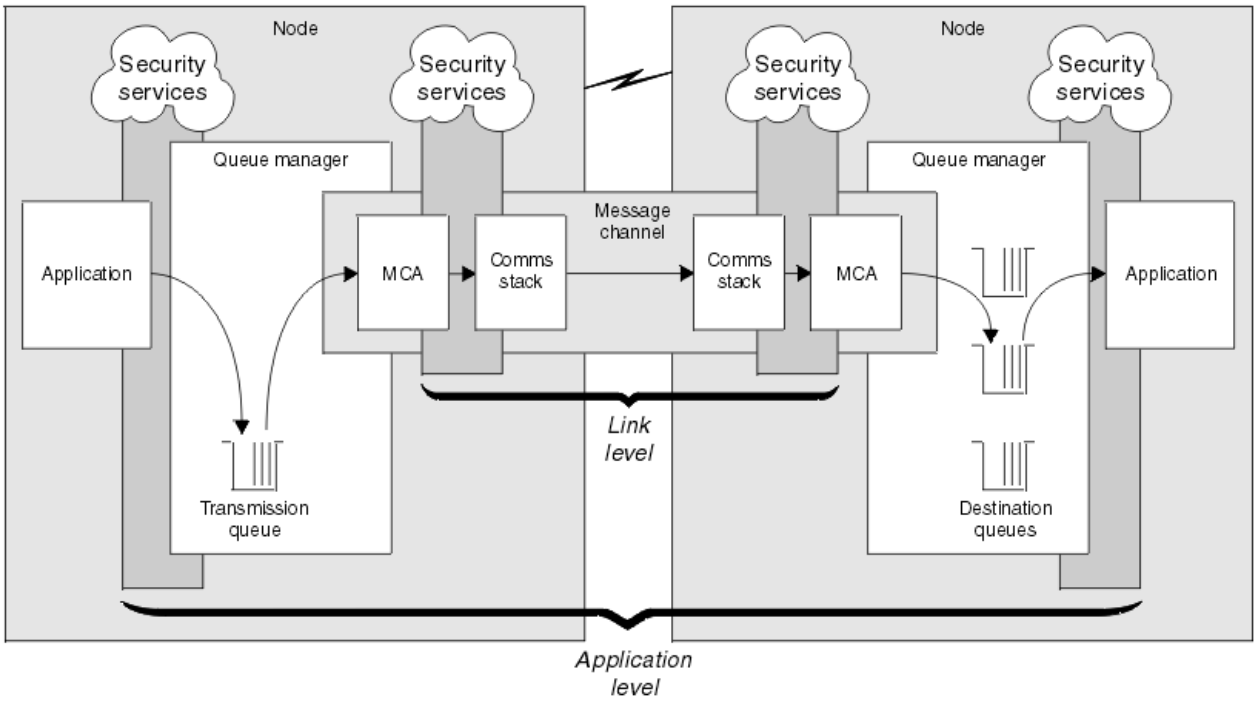
“Ukončovací programy kanálu” na stránce 104
Ukončovací programy kanálu jsou programy, které jsou volány v definovaných místech v posloupnosti zpracování agenta MCA. Uživatelé a dodavatelé mohou napsat své vlastní uživatelské programy kanálu. Některé jsou dodávány produktem IBM.

“Zabezpečení kanálů pomocí SSL/TLS” na stránce 110
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 odkazů a zabezpečení na úrovni aplikace

Toto téma obsahuje informace o různých aspektech zabezpečení na úrovni odkazů a zabezpečení na úrovni aplikací a porovnává dvě úrovně zabezpečení.

Úroveň odkazu a zabezpečení na úrovni aplikace jsou popsány v tématu Obrázek 10 na stránce 99.



Obrázek 10. Zabezpečení na úrovni odkazů a zabezpečení na úrovni aplikace

Ochrana zpráv ve frontách

Zabezpečení na úrovni linky může chránit zprávy, zatímco jsou přenášeny z jednoho správce front do jiného. Je zvláště důležité, když jsou zprávy přenášeny přes nezabezpečenou síť. Nemůže však chránit zprávy, dokud jsou uloženy ve frontách buď ve zdrojovém správci front, v cílovém správci front, nebo ve středním správci front.

z/OS V 9.2.0 z/OS šifrování datové sady může poskytovat určitou ochranu zpráv uložených ve frontách, ale pouze pro data, která jsou uložena v lokálním správci front. Informace naleznete v části Důvěrnost dat v produktu IBM MQ for z/OS s šifrováním datové sady. Další informace viz.

Zabezpečení na úrovni aplikace může díky porovnání chránit zprávy, zatímco jsou uloženy ve frontách a platí i v případě, že se nepoužívá distribuované řazení do fronty. To je hlavní rozdíl mezi úrovní zabezpečení na úrovni zabezpečení a zabezpečením na úrovni aplikace a ilustrovat se v části Obrázek 10 na stránce 99.

Správci front nejsou spuštění v řízeném a důvěryhodném prostředí

Je-li správce front spuštěn v řízeném a důvěryhodném prostředí, mohou být mechanizmy řízení přístupu poskytované produktem IBM MQ považovány za dostatečné k ochraně zpráv uložených ve frontách. To platí zvláště v případě, že je zahrnuto pouze lokální řazení do fronty a zprávy nikdy neopustí správce front. Zabezpečení na úrovni aplikace v tomto případě může být považováno za zbytečné.

Zabezpečení na úrovni aplikace může být také považováno za zbytečné, pokud jsou zprávy přenášeny do jiného správce front, který je také spuštěn v řízeném a důvěryhodném prostředí, nebo jsou tyto zprávy přijaty od takového správce front. Potřeba zabezpečení na úrovni aplikace se stává větší, když jsou zprávy přenášeny nebo přijímány od správce front, který není spuštěn v řízeném a důvěryhodném prostředí.

Rozdíly v nákladech

Zabezpečení na úrovni aplikace může stát více než zabezpečení na úrovni odkazů, pokud jde o administraci a výkon.

Náklady na administraci budou pravděpodobně větší, protože existují potenciálně více omezení pro konfiguraci a údržbu. Můžete například chtít zajistit, aby konkrétní uživatel odesílal pouze určité typy zpráv a odesílal zprávy pouze do určitých míst určení. A naopak, možná budete muset zajistit, aby určitý uživatel přijímal pouze určité typy zpráv a přijímal zprávy pouze z určitých zdrojů. Místo správy služeb zabezpečení na úrovni propojení na jednom kanálu zpráv může být třeba konfigurovat a spravovat pravidla pro každou dvojici uživatelů, kteří si vyměňují zprávy v rámci daného kanálu.

Je-li služba zabezpečení vyvolána pokaždé, když aplikace vloží nebo obdrží zprávu, může dojít k ovlivnění výkonu.

Organizace mají tendenci uvažovat o zabezpečení na úrovni odkazů jako první, protože by mohlo být jednodušší implementovat. Zváží zabezpečení na úrovni aplikace, pokud zjistí, že zabezpečení na úrovni odkazů nesplňuje všechny jejich požadavky.

Dostupnost komponent

Obecně platí, že v distribuovaném prostředí služba zabezpečení vyžaduje komponentu na minimálně dvou systémech. Například, zpráva může být šifrována na jednom systému a dešifrována na jiném systému. To platí jak pro zabezpečení na úrovni odkazů, tak pro zabezpečení na úrovni aplikace.

V heterogenním prostředí s různými platformami, z nichž každá má různé úrovně zabezpečení, nemusí být požadované komponenty služby zabezpečení dostupné pro každou platformu, na které jsou potřeba, a v podobě, kterou lze snadno použít. Pravděpodobně se jedná o spíše problém zabezpečení na úrovni aplikace než zabezpečení na úrovni odkazů, a to zejména v případě, že máte v úmyslu poskytovat vlastní zabezpečení na úrovni aplikací prostřednictvím nákupu v komponentách z různých zdrojů.

Zprávy ve frontě nedoručených zpráv

Je-li zpráva chráněna zabezpečením na úrovni aplikace, může dojít k problému, pokud zpráva z nějakého důvodu nedosáhne místa určení a je vložena do fronty nedoručených zpráv. Pokud nemůžete pracovat na tom, jak zpracovat zprávu z informací v deskriptoru zpráv a záhlaví zablokovaných dopisů, může být nutné zkontrolovat obsah dat aplikace. Tuto akci nelze provést, pokud jsou data aplikace šifrována a může ji dešifrovat pouze určený příjemce.

Co zabezpečení na úrovni aplikace nelze provést

Zabezpečení na úrovni aplikace není kompletní řešení. I když implementujete zabezpečení na úrovni aplikací, můžete stále ještě vyžadovat některé služby zabezpečení na úrovni odkazů. Příklad:

- Když se spustí kanál, vzájemné ověření těchto dvou jednotek MCA může být stále ještě požadavek. To lze provést pouze pomocí služby zabezpečení na úrovni odkazu.
- Zabezpečení na úrovni aplikace nemůže ochránit záhlaví přenosové fronty, MQXQH, které obsahuje vložený deskriptor zprávy. Stejně tak nemůže chránit data v jiných tocích protokolu kanálu produktu IBM MQ než data zpráv. Tuto ochranu mohou poskytnout pouze zabezpečení na úrovni odkazů.

- Pokud jsou služby zabezpečení na úrovni aplikace vyvolány na konci kanálu serveru MQI, služby nemohou chránit parametry volání MQI, která jsou odesílána přes kanál. Data aplikací v rámci volání MQPUT, MQPUT1nebo MQGET jsou však nechráněná. Ochranu může v tomto případě zajistit pouze zabezpečení na úrovni odkazů.

zabezpečení na úrovni odkazů

Zabezpečení na úrovni odkazu odkazuje na tyto služby zabezpečení, které jsou přímo nebo nepřímo vyvolány agentem MCA, komunikačním subsystémem nebo kombinací těchto dvou činností.

Zabezpečení na úrovni odkazu je ilustrováno v Obrázek 10 na stránce 99.

Zde je několik příkladů služeb zabezpečení na úrovni odkazu:

- Agent MCA na každém konci kanálu zpráv může ověřit jeho partnera. To se provádí při spuštění kanálu a bylo ustanoveno komunikační spojení, ale před zahájením toku zpráv. Pokud dojde k selhání ověření na každém konci, kanál se zavře a žádné zprávy se nepřenášejí. Toto je příklad identifikace a ověřovací služby.
- Zprávu lze šifrovat na odesílající straně kanálu a dešifrována na přijímajícím konci. Toto je příklad služby důvěrnosti.
- Na přijímajícím konci kanálu může být zkontrolována zpráva s cílem určit, zda byl její obsah během přenosu po síti úmyslně změněn. Toto je příklad služby integrity dat.

Zabezpečení na úrovni odkazu poskytované produktem IBM MQ

Primárním prostředkem pro zajištění důvěrnosti a integrity dat v produktu IBM MQ je použití TLS. Další informace o použití TLS v produktu IBM MQviz “Protokoly zabezpečení TLS v produktu IBM MQ” na stránce 22. Pro ověření poskytuje produkt IBM MQ zařízení k použití záznamů ověření kanálu. Záznamy ověření kanálu nabízejí přesnou kontrolu nad přístupem udělenou připojujícím se systémům na úrovni jednotlivých kanálů nebo skupin kanálů. Další informace viz “Záznamy ověření kanálu” na stránce 47.

Poskytnutí zabezpečení na úrovni vlastního odkazu

Můžete poskytnout své vlastní služby zabezpečení na úrovni odkazů. Vytvoření vlastních ukončovacích programů kanálu je hlavní způsob, jak poskytovat vlastní služby zabezpečení na úrovni propojení.

Uživatelské programy kanálu jsou představeny v produktu “Ukončovací programy kanálu” na stránce 104. Stejné téma také popisuje ukončovací program kanálu, který je dodáván s programem IBM MQ for Windows (uživatelským programem kanálu SSPI). Tento výstupní program kanálu je dodáván ve zdrojovém formátu, takže je možné upravit zdrojový kód tak, aby vyhovoval vašim požadavkům. Pokud tento výstupní program kanálu nebo výstupní programy kanálu dostupné od jiných dodavatelů nesplňují vaše požadavky, můžete navrhnout a napsat vlastní. Toto téma obsahuje návrhy způsobů, jak mohou uživatelské programy kanálu poskytovat služby zabezpečení. Informace o tom, jak zapisovat ukončovací program kanálu, najdete v tématu Psaní programů ukončovacích programů.

Zabezpečení na úrovni odkazu pomocí uživatelské procedury zabezpečení

Uživatelské procedury zabezpečení normálně pracují ve dvojicích; jedna na každém konci kanálu. Zavolají se ihned po dokončení počátečního vyjednávání dat při spuštění kanálu.

Uživatelské procedury zabezpečení lze použít k poskytnutí identifikace a ověření, přístupu k řízení přístupu a důvěrnosti.

Zabezpečení na úrovni odkazu pomocí uživatelské procedury pro zprávy

Ukončení zprávy lze použít pouze v kanálu zpráv, nikoli v kanálu MQI. Má přístup k záhlaví přenosové fronty, MQXQH, které obsahuje vložený deskriptor zpráv, a data aplikace ve zprávě. Může upravovat obsah zprávy a měnit jeho délku.

Ukončení zprávy lze použít pro jakýkoli účel, který vyžaduje přístup k celé zprávě, spíše než její části.

Uživatelské procedury pro zprávy lze použít k poskytnutí identifikace a ověření, řízení přístupu, důvěrnosti, integrity dat a neodmítání, a z jiných důvodů než zabezpečení.

Zabezpečení na úrovni odkazu pomocí uživatelských procedur pro odesílání a příjem
Uživatelské procedury pro odesílání a příjem lze použít na obou zprávách i v kanálech MQI. Jsou volány pro všechny typy dat, které proudí na kanálu, 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 je v kanálu zpráv potřeba sběrnice MCA rozdělit zprávu a odeslat ji ve více než jednom segmentu přenosu, je volaná uživatelská procedura pro odeslání volána pro každý přenosový segment obsahující část zprávy a na přijímajícím konci je volána uživatelská procedura pro příjem pro každý segment přenosu. Pokud jsou vstupní nebo výstupní parametry volání MQI příliš velké na to, aby mohly být odeslány v rámci jednoho segmentu přenosu, dojde ke stejnému výsledku.

Na kanálu MQI označuje bajt 10 pro segment přenosu volání MQI a udává, zda segment přenosu obsahuje vstupní nebo výstupní parametry volání. Uživatelské procedury pro odesílání a příjem mohou zkoumat tento bajt a určit, zda volání MQI obsahuje data aplikací, která mohou být chráněna.

Je-li uživatelská procedura pro odeslání volána poprvé, získá a inicializuje všechny prostředky, které potřebuje, může požádat agenta MCA o vyhrazení zadaného množství prostoru ve vyrovnávací paměti, který obsahuje segment přenosu. Když je později volán ke zpracování segmentu přenosu, může použít tento prostor k přidání zašifrovaného klíče nebo digitálního podpisu, například. Odpovídající výstupní bod příjmu na druhém konci kanálu může odebrat data přidaná uživatelskou procedurou odeslání a použít ji ke zpracování segmentu přenosu.

Uživatelské procedury pro odesílání a příjem jsou nejvhodnější pro účely, v nichž nemusí rozumět struktuře dat, které zpracovávají, a mohou proto přistupovat ke každému segmentu přenosu jako s binárním objektem.

Uživatelské procedury pro odesílání a příjem lze použít k zajištění utajení a integrity dat a k použití jiných než zabezpečení.

Související úlohy

Identifikace volání rozhraní API v ukončovacím programu pro odeslání nebo přijetí

zabezpečení na úrovni aplikace

Zabezpečení na úrovni aplikace odkazuje na ty služby zabezpečení, které jsou vyvolány na rozhraní mezi aplikací a správcem front, ke kterému je připojena.

Tyto služby jsou vyvolány, když aplikace odesílá volání MQI do správce front. Služby mohou být vyvolány přímo nebo nepřímo aplikací, správcem front, jiným produktem, který podporuje produkt IBM MQ, nebo kombinací libovolné z těchto pracovních procesů. Zabezpečení na úrovni aplikace je ilustrováno v tématu Obrázek 10 na stránce 99.

Zabezpečení na úrovni aplikace je také označováno jako *koncový-konec zabezpečení* nebo *zabezpečení na úrovni zpráv*.

Zde je několik příkladů služeb zabezpečení na úrovni aplikace:

- Když aplikace vloží zprávu do fronty, deskriptor zprávy obsahuje ID uživatele přidružené k aplikaci. Avšak zde nejsou přítomna žádná data, jako je zašifrované heslo, které lze použít k ověření ID uživatele. Tato data mohou přidávat služba zabezpečení. Když je zpráva nakonec načtena přijímající aplikací, další komponenta služby může autentizovat ID uživatele pomocí dat, která cestovala se zprávou. Toto je příklad identifikace a ověřovací služby.
- Zprávu lze zašifrovat, když je vložena do fronty aplikací a dešifrována, když je načtena přijímající aplikací.Toto je příklad služby důvěrnosti.
- Zpráva může být zkontrolována, když je načtena přijímající aplikací. Tato kontrola určuje, zda jeho obsah byl úmyslně upraven od té doby, kdy byla poprvé vložena do fronty odesílající aplikací.Toto je příklad služby integrity dat.

Plánování pro databázi Advanced Message Security
Advanced Message Security (AMS) je komponenta produktu IBM MQ , která poskytuje vysokou úroveň ochrany citlivých dat procházejících přes síť IBM MQ , a to bez dopadu na koncové aplikace.

Pokud přesouváte vysoce citlivé nebo cenné informace, zejména důvěrné informace nebo informace související s platbami, jako jsou záznamy pacientů nebo podrobnosti o kreditní kartě, musíte věnovat zvláštní pozornost zabezpečení informací. Zajištění toho, aby byly informace pohybující se kolem podniku zachovány jeho integrity a chráněny před neoprávněným přístupem, je pokračující výzvou a zodpovědností. Pravděpodobně se budete muset řídit bezpečnostními předpisy, a to s rizikem sankcí za nedodržování norem.

Můžete vyvinout vlastní rozšíření zabezpečení na produkt IBM MQ. Tato řešení však vyžadují specializované dovednosti a mohou být složité a nákladné udržovat. Produkt Advanced Message Security pomáhá řešit tyto problémy při přesouvání informací v podniku prakticky ve všech typech komerčních informačních systémů.

Produkt Advanced Message Security rozšiřuje funkce zabezpečení produktu IBM MQ následujícími způsoby:

- Poskytuje ochranu dat na úrovni aplikací a koncových bodů pro infrastrukturu systému zpráv s cílem použít buď šifrování, nebo digitální podepisování zpráv.
- Poskytuje komplexní zabezpečení, aniž by bylo nutné psát komplexní kód zabezpečení nebo upravovat či opětovně kompilovat existující aplikace.
- Využívá technologii PKI (Public Key Infrastructure) k zajištění služeb ověření, autorizace, utajení a integrity dat pro zprávy.
- Poskytuje administraci zásad zabezpečení pro sálové počítače a distribuované servery.
- Podporuje jak IBM MQ servery, tak klienty.
- Poskytuje integraci s produktem Managed File Transfer pro poskytování řešení zabezpečeného systému zpráv typu end-to-end.

Další informace viz “Advanced Message Security” na stránce 581.

Zajištění vlastního zabezpečení na úrovni aplikace
Můžete poskytnout své vlastní služby zabezpečení na úrovni aplikace. Pro usnadnění implementace zabezpečení na úrovni aplikací poskytuje produkt IBM MQ dva uživatelské procedury, uživatelské procedury rozhraní API a ukončení přejezdu rozhraní API.

Uživatelská procedura rozhraní API a uživatelská procedura překřížení rozhraní API mohou poskytovat identifikaci a ověření, řízení přístupu, utajení, integritu dat a služby neodmítání a další funkce nesouvisející se zabezpečením.

Není-li uživatelská procedura rozhraní API nebo uživatelská procedura překřížení rozhraní API podporována ve vašem systémovém prostředí, možná byste měli zvážit i jiné způsoby poskytování vaší vlastní zabezpečení na úrovni aplikací. Jedním ze způsobů je vyvinout rozhraní API vyšší úrovně, které zapouzdří rozhraní MQI. Programátoři pak pomocí tohoto rozhraní API namísto rozhraní MQI zapisují aplikace produktu IBM MQ .

Nejběžnější důvody použití rozhraní API vyšší úrovně jsou:

- Chcete-li skrýt rozšířené funkce rozhraní MQI od programátorů, postupujte takto:
- Chcete-li vynutit standardy při použití rozhraní MQI, postupujte takto:
- Přidání funkce do MQI. Tato dodatečná funkce může být službami zabezpečení.

Některé produkty dodavatelů používají tuto techniku k zajištění zabezpečení na úrovni aplikací pro produkt IBM MQ.

Plánujete-li poskytovat služby zabezpečení tímto způsobem, uvědomte si následující údaje týkající se konverze dat:

- Pokud byl do aplikační dat ve zprávě přidán token zabezpečení, jako je například digitální podpis, musí být jakýkoli kód provádějící převod dat vědom přítomnosti tohoto tokenu.
- Token zabezpečení mohl být odvozen z binárního obrazu dat aplikace. Proto každá kontrola tokenu musí být provedena před převodem dat.
- Pokud byla data aplikace ve zprávě šifrována, musí být dešifrována před převodem dat.

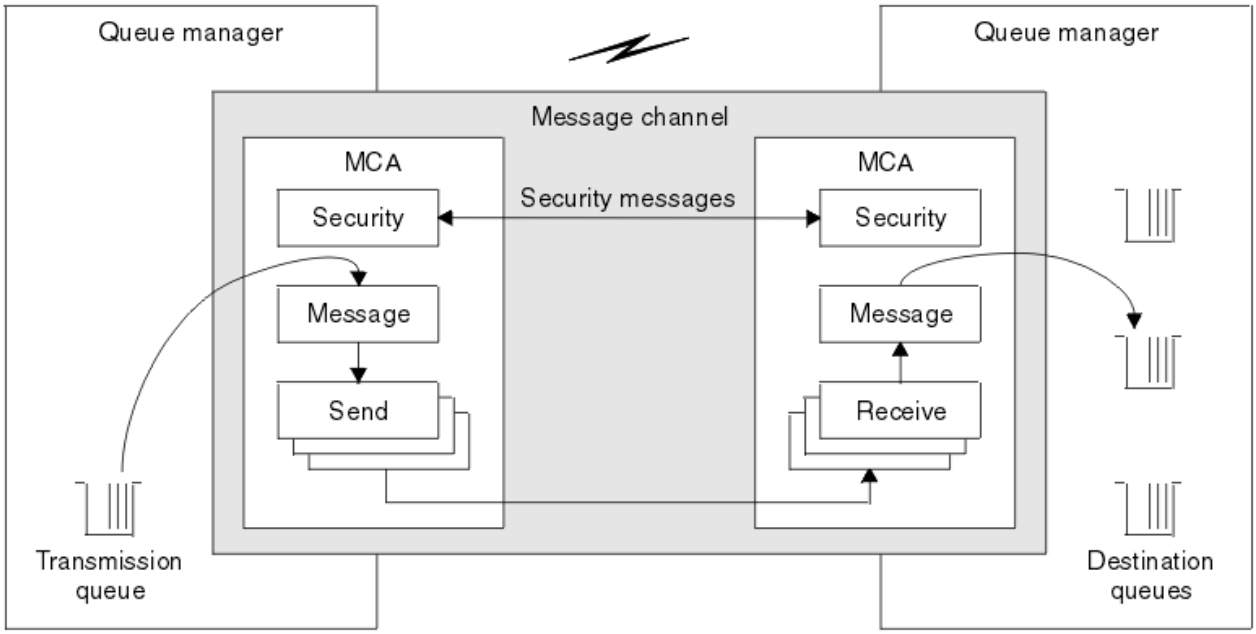
Ukončovací programy kanálu

Ukončovací programy kanálu jsou programy, které jsou volány v definovaných místech v posloupnosti zpracování agenta MCA. Uživatelé a dodavatelé mohou napsat své vlastní uživatelské programy kanálu. Některé jsou dodávány produktem IBM.

Existuje několik typů ukončovacích programů kanálu, ale pouze čtyři mají roli při poskytování zabezpečení na úrovni odkazu:

- Uživatelská procedura pro zabezpečení zprávy
- Ukončení zprávy
- Ukončení odeslání
- Ukončení příjmu

Tyto čtyři typy ukončovacího programu kanálu jsou popsány v tématu Obrázek 11 na stránce 104 a jsou popsány v následujících tématech.



Obrázek 11. Uživatelské procedury zabezpečení, zprávy, odeslání a přijetí na kanálu zpráv

Související pojmy

Kanály-uživatelské programy pro kanály systému zpráv

Přehled uživatelské procedury zabezpečení

Uživatelské procedury zabezpečení normálně pracují ve dvojicích. Jsou volány před tokem zpráv a jejich účelem je umožnit agentovi MCA ověření jeho partnera.

Uživatelské procedury zabezpečení obvykle pracují ve dvojicích; jedna na každém konci kanálu. Jsou volány ihned po dokončení počátečního vyjednávání dat při spuštění kanálu, ale předtím, než začnou být odesílány zprávy. Primárním účelem uživatelské procedury zabezpečení je umožnit agentovi MCA na každém konci kanálu ověřovat jeho partnera. Avšak neexistuje nic, co by bránilo ukončení zabezpečení z provádění jiné funkce, dokonce i funkce, která nemá nic společného se zabezpečením.

Uživatelské procedury zabezpečení mohou vzájemně komunikovat odesláním *zpráv zabezpečení*. Formát zprávy zabezpečení není definován a je určován uživatelem. Jeden možný výsledek výměny zpráv zabezpečení je takový, že jedna z uživatelských procedur zabezpečení může rozhodnout, že nebude pokračovat dále. V takovém případě je kanál uzavřen a zprávy nevedou k toku. Pokud existuje uživatelská procedura zabezpečení pouze na jednom konci kanálu, je tato uživatelská procedura stále volána a může se rozhodnout, zda má kanál pokračovat, nebo zavřít kanál.

Uživatelské procedury zabezpečení lze volat pro kanály zpráv i pro kanály MQI. Název uživatelské procedury zabezpečení je určen jako parametr v definici kanálu na každém konci kanálu.

Další informace o uživatelských procedurách zabezpečení najdete v tématu "Zabezpečení na úrovni odkazu pomocí uživatelské procedury zabezpečení" na stránce 101.

Ukončení zprávy

Uživatelské procedury pro zprávy pracují pouze na kanálech zpráv a normálně pracují ve dvojicích. Ukončení zprávy může pracovat na celé zprávě a provádět na něm různé změny.

Ukončení zpráv na konci odesílání a přijímání konců kanálu obvykle pracuje ve dvojicích. Uživatelská procedura pro odeslání zprávy na odesílajícím konci kanálu je volána poté, co program MCA obdržel zprávu z přenosové fronty. Na přijímajícím konci kanálu je uživatelská procedura pro zprávy volána před tím, než agent MCA vloží zprávu do cílové fronty.

Uživatelská procedura pro zprávy má přístup k záhlaví přenosové fronty, MQXQH, které obsahuje vložený deskriptor zpráv, a data aplikace ve zprávě. Uživatelská procedura pro zprávy může upravit obsah zprávy a změnit jeho délku. Změna délky může být výsledkem komprimace, dekomprimace, šifrování nebo dešifrování zprávy. Může se také jednat o výsledek přidání dat do zprávy nebo o odebrání dat z ní.

Uživatelské procedury pro zprávy lze použít k jakémukoli účelu, který vyžaduje přístup k celé zprávě, nikoli jeho části, a ne nezbytně pro zabezpečení.

Ukončení zprávy může určit, že zpráva, kterou momentálně zpracovává, by neměla dále směřovat ke svému cíli. Agent MCA poté vloží zprávu do fronty nedoručených zpráv. Ukončení kanálu může také zavřít okno ukončení zprávy.

Uživatelské procedury pro zprávy lze volat pouze v kanálech zpráv, nikoli v kanálech MQI. Důvodem je to, že účelem kanálu MQI je povolit vstupní a výstupní parametry volání MQI pro tok mezi aplikací produktu IBM MQ MQI client a správcem front.

Název uživatelské procedury pro zprávy je určen jako parametr v definici kanálu na každém konci kanálu. Můžete také zadat seznam uživatelských procedur, které mají být spouštěny za dědění.

Další informace o uživatelských procedurách pro zprávy naleznete v tématu "Zabezpečení na úrovni odkazu pomocí uživatelské procedury pro zprávy" na stránce 101.

Odeslat a přijmout uživatelské procedury

Uživatelské procedury pro odesílání a příjem obvykle pracují ve dvojicích. Pracují na převodových segmentech a nejlépe se používají tam, kde struktura dat, která zpracovává, není relevantní.

Uživatelská procedura odeslání na jednom konci kanálu a *uživatelská procedura příjmu* na druhém konci normálně pracují ve dvojicích. Uživatelská procedura pro odeslání zprávy je volána těsně před tím, než program MCA odešle oznámení o odeslání dat prostřednictvím komunikačního spojení. Uživatelská procedura pro příjem je volána bezprostředně poté, co agent MCA znovu získá řízení po přijetí komunikace a přijal data z komunikačního připojení. Je-li sdílení konverzací v použití kanálu MQI, je pro každou konverzaci volána jiná instance uživatelské procedury odeslání a přijetí.

Toky protokolu kanálu produktu IBM MQ mezi dvěma jednotkami MCAs v kanálu zpráv obsahují řídicí informace a také data zprávy. Podobně u kanálu MQI obsahují toky informace o řízení spolu s parametry volání MQI. Uživatelské procedury pro odesílání a příjem jsou volány pro všechny typy dat.

Data zprávy tečou pouze v jednom směru kanálu zpráv, ale na kanálu MQI se vstupní parametry toku volání MQI v jednom směru a výstupní parametry toku v druhém směru ubíjí. V případě kanálů zpráv i kanálů MQI lze řídit toky informací v obou směrech. V důsledku toho lze volat a přijímat uživatelské procedury na obou koncích kanálu.

Jednotka dat, která je přenášena v jednom toku mezi dvěma MCAs, se nazývá *transmission 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 segmentu přenosu. Těchto 8 bajtů tvoří část záhlaví protokolu kanálu IBM MQ . Existují také omezení, jak velká uživatelská procedura pro odeslání může zvýšit délku přenosového segmentu.

Zejména odeslání uživatelské procedury odeslání nemůže zvýšit svou délku nad maximum, které bylo vyjednán mezi dvěma MCAs při spuštění kanálu.

Je-li v kanálu zpráv příliš velká zpráva, která má být odeslána v rámci jednoho přenosového segmentu, odesílající agent MCA rozdělí zprávu a odešle ji ve více než jednom segmentu přenosu. V důsledku toho je pro každý segment přenosu obsahující část zprávy volána uživatelská procedura odeslání a na přijímajícím konci je volána uživatelská procedura pro přijetí zprávy pro každý segment přenosu. Přijímající agent MCA znovu tvoří zprávu z přenosových segmentů poté, co byly zpracovány uživatelskou procedurou pro přijetí zprávy.

Podobně u 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 v případě volání MQPUT, MQPUT1nebo MQGET, pokud jsou data aplikace dostatečně velká.

Vezmeme-li tyto úvahy v úvahu, je vhodnější použít pro účely odeslání a přijetí uživatelské procedury, které nepotřebují rozumět struktuře dat, které zpracovávají, a mohou proto přistupovat ke každému segmentu přenosu jako k binárnímu objektu.

Odesílatel nebo přijímací procedura může zavřít kanál.

Názvy uživatelské procedury odeslání a ukončení příjmu jsou uvedeny jako parametry v definici kanálu na každém konci kanálu. Můžete také uvést seznam uživatelských procedur odeslání, které mají být spuštěny v posloupnosti. Podobně můžete zadat seznam ukončení příjmu.

Další informace o uživatelských procedurách pro odesílání a příjem naleznete v příručce “Zabezpečení na úrovni odkazu pomocí uživatelských procedur pro odesílání a příjem” na stránce 102.

Plánování integrity dat

Naplánujte, jak zachovat integritu vašich dat.

Integritu dat můžete implementovat na úrovni aplikace nebo na úrovni odkazů.

Na úrovni aplikace můžete použít výstupní programy rozhraní API, pokud standardní zařízení nevyhovují vašim požadavkům. Můžete se rozhodnout použít produkt Advanced Message Security (AMS) k digitálnímu podpisu zpráv za účelem ochrany proti neautorizované úpravě.

Na úrovni linky se můžete rozhodnout použít TLS, v takovém případě musíte naplánovat použití digitálních certifikátů. Ukončovací programy kanálu můžete také použít, pokud standardní vybavení nevyhovují vašim požadavkům.

Související pojmy

“Zabezpečení kanálů pomocí SSL/TLS” na stránce 110
Podpora TLS v produktu IBM MQ používá objekt ověřovacích informací správce front a různé příkazy MQSC. Musíte také zvážit použití digitálních certifikátů.

“Integrita dat v produktu IBM MQ” na stránce 21
Službu integrity dat můžete použít ke zjištění, zda byla zpráva upravena.

“Plánování pro databázi Advanced Message Security” na stránce 102
Advanced Message Security (AMS) je komponenta produktu IBM MQ , která poskytuje vysokou úroveň ochrany citlivých dat procházejících přes síť IBM MQ , a to bez dopadu na koncové aplikace.

Související odkazy

Popis uživatelské procedury rozhraní

Volání uživatelských procedur kanálů a datové struktury

Plánování monitorování

Rozhodněte se, která data budete potřebovat k monitorování, a jak zachytíte a zpracujete informace o auditu. Zvažte, jak zkontrolovat, zda je systém správně nakonfigurovaný.

Existuje několik aspektů monitorování aktivity. Aspekty, které musíte vzít v úvahu, jsou často definovány požadavky auditora, a tyto požadavky jsou často řízeny regulačními standardy, jako jsou HIPAA (Health

Insurance Portability and Accountability Act) nebo SOX (Sarbanes-Oxley). Produkt IBM MQ poskytuje funkce určené k pomoci s dodržováním těchto standardů.

Zvažte, zda máte zájem pouze o výjimky nebo o to, zda se zajímáte o veškeré chování systému.

Některé aspekty auditu lze také považovat za provozní monitorování; jedno rozlišování pro audit je takové, že se často díváte na historická data, nejen při pohledu na výstrahy v reálném čase. Monitorování je zahrnuto v sekci Monitorování a výkon.

Jaká data se mají monitorovat

Zvažte, jaké typy dat nebo činností je třeba monitorovat, jak je popsáno v následujících sekcích:

Změny provedené v produktu IBM MQ pomocí rozhraní produktu IBM MQ
Konfigurujte produkt IBM MQ , chcete-li vydat události přípravy nástrojů, zejména události příkazů a události konfigurace.

Změny provedené v produktu IBM MQ mimo jeho ovládací prvek
Některé změny mohou ovlivnit chování produktu IBM MQ , ale nelze je přímo monitorovat produktem IBM MQ. Příklady takových změn zahrnují změny v konfiguračních souborech `mqs.ini`, `qm.inia` `mqclient.ini`, vytváření a odstraňování správců front, instalaci binárních souborů, jako jsou uživatelské programy, a změny oprávnění k souboru. Chcete-li monitorovat tyto aktivity, musíte použít nástroje spuštěné na úrovni operačního systému. Jsou k dispozici různé nástroje a jsou vhodné pro různé operační systémy. Můžete také mít protokoly vytvořené přidruženými nástroji, jako je například *sudo*.

Provozní řízení IBM MQ
Je možné, že budete muset použít nástroje operačního systému k monitorování aktivit, jako je spouštění a zastavování správců front. V některých případech může být produkt IBM MQ nakonfigurován k vydávání událostí přípravy nástrojů.

Aktivita aplikace v rámci produktu IBM MQ
Chcete-li monitorovat akce aplikací, například otevírání front a vkládání zpráv a získávání zpráv, nakonfigurujte produkt IBM MQ tak, aby vydal odpovídající události.

Výstrahy nepravdivosti
Chcete-li provést audit při pokusu o narušení zabezpečení, nakonfigurujte systém tak, aby vydal události autorizace. Události kanálu mohou být užitečné také k zobrazení aktivity, zvláště pokud je kanál neočekávaně ukončen.

Plánování zachytávání, zobrazení a archivace dat auditu

Řadu z prvků, které potřebujete, jsou nahlášeny jako zprávy událostí produktu IBM MQ . Musíte vybrat nástroje, které mohou tyto zprávy číst a formátovat. Pokud se zajímáte o dlouhodobé uložení a analýzu, musíte je přesunout do pomocného úložného mechanizmu, jako je například databáze. Pokud tyto zprávy nezpracovávají, zůstanou ve frontě událostí a pravděpodobně budou zaplňovat frontu. Můžete se rozhodnout implementovat nástroj, který automaticky provede akce na základě některých událostí; chcete-li například vydat výstrahu, dojde-li k selhání zabezpečení.

Ověření, že je systém správně nakonfigurován

Sada testů se dodává spolu s IBM MQ Explorer. Použijte tyto informace ke kontrole problémů v definicích objektů.

Také pravidelně kontrolujte, že konfigurace systému je taková, jakou očekáváte. Ačkoli může příkaz a události konfigurace hlásit, kdy se něco změnilo, 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 výběrového vysílání a při použití brány firewall.

Další informace naleznete v následujících dílčích tématech:

Ověřování kanálu

Pokud odešlete nebo obdržíte zprávu prostřednictvím kanálu, musíte poskytnout přístup k různým prostředkům produktu IBM MQ . Agenti MCA (Message Channel Agents) jsou v podstatě IBM MQ aplikací, které přesouvají zprávy mezi správci front a jako takové vyžadují přístup k různým prostředkům produktu IBM MQ , aby fungovaly správně.

Chcete-li přijímat zprávy v čase PUT pro MCA, můžete použít buď ID uživatele přidružené k agentovi MCA, nebo ID uživatele přidružené ke zprávě.

V čase CONNECT můžete namapovat ID uživatele na alternativního uživatele pomocí ověřovacích záznamů kanálu produktu **CHLAUTH** .

V produktu IBM MQmohou být kanály chráněny pomocí TLS podpory.

ID uživatelů přidružená k odesílání a přijímání kanálů, kromě odesílacího kanálu, kde je atribut MCAUSER nepoužívaný, vyžaduje 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, které jsou vyžadovány uživatelskými procedurami kanálu.
- ID uživatele MCAUSER přijímacího kanálu potřebuje oprávnění *+ setall* . Důvod spočívá v tom, že přijímací kanál musí vytvořit celý MQMD, včetně všech polí kontextu, pomocí dat přijatých ze vzdáleného odesílacího kanálu. Správce front proto vyžaduje, aby uživatel provádějící tuto aktivitu měl oprávnění *+ setall* . Toto oprávnění *+ setall* musí být uděleno uživateli pro:
  - Všechny fronty, do kterých kanál příjemce validly umísťuje zprávy.
  - Objekt správce front. Další informace viz téma Autorizace pro kontext.
- ID uživatele MCAUSER přijímacího kanálu, kde odesílatel požádal o zprávu hlášení COA, potřebuje oprávnění *+ passid* přenosové fronty, která vrací zprávu hlášení. Bez tohoto oprávnění se protokolují chybové zprávy AMQ8077 .
- S ID uživatele asociovaným s přijímajícím kanálem můžete otevřít cílové fronty pro vkládání zpráv do front. To zahrnuje rozhraní MQI (Message Queuing Interface), takže mohou být provedeny další kontroly řízení přístupu, pokud nepoužíváte produkt IBM MQ Object Authority Manager (OAM). Můžete uvést, zda jsou kontroly autorizace provedeny proti ID uživatele přidruženému ke zprávě MCA (jak je popsáno v tomto tématu), nebo proti ID uživatele přidruženému ke zprávě (z pole MQMD UserIdentifier).

  U typů kanálů, na které se vztahuje, určuje parametr **PUTAUT** definice kanálu, které ID uživatele se použije pro tyto kontroly.
  - Výchozí nastavení kanálu je použití účtu služby správce front, který má úplná administrativní práva a nevyžaduje žádné speciální autorizace.
  - V případě kanálů připojení serveru jsou administrativní připojení standardně blokována podle pravidel CHLAUTH a vyžadují explicitní zajišťování.
  - Kanály typu receiver receiver, requester a cluster-receiver allow local administration by any adjacent queue manager, unless the administrator takes steps to restrict this access.
  - Není nutné udělovat oprávnění *dsp* a *ctrlx* pro ID uživatele MCAUSER přijímacího kanálu.
  - Pokud před IBM MQ 8.0.0 Fix Pack 4použijete ID uživatele, které nemá oprávnění k administraci produktu IBM MQ , musíte pro kanál k práci udělit oprávnění **dsp** a **ctrlx** pro kanál k tomuto ID uživatele.

    V produktu IBM MQ 8.0.0 Fix Pack 4neexistují žádné kontroly oprávnění, když se kanál znovu synchronizuje a opravuje pořadová čísla.

    Nicméně zadání příkazu RESET CHANNEL ručně stále vyžaduje **+dsp** a **+ctrlx** ve všech vydáních.

    Upozornění: Je-li pro potvrzení dávky zpráv zapotřebí resetování kanálu, produkt IBM MQ se pokusí o dotaz na kanál, který vyžaduje oprávnění správce **+dsp** .
  - Atribut MCAUSER se nepoužívá pro typ kanálu SDR.

– Použijete-li 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 vydat pro udělení oprávnění k 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 agentovi MCA závisí na typu agenta MCA. Existují dva typy MCA:

MCA volajícího
MCA, které iniciují kanál. MCAs volajícího lze spustit jako jednotlivé procesy, jako podprocesy iniciátoru kanálu nebo jako podprocesy fondu procesů. Použité ID uživatele je ID uživatele přidružené k nadřízenému procesu (inicializátor kanálu) nebo ID uživatele přidružené k procesu, který spouští agenta MCA.

MCA-odpovědní
Responder MCAs jsou MCAs, které jsou spuštěny jako výsledek požadavku volajícím MCA. Kontrolovací jednotky MCU mohou být spuštěny jako jednotlivé procesy, jako podprocesy modulu listener, nebo jako podprocesy fondu procesů. ID uživatele může být libovolný z následujících typů (v tomto pořadí preferencí):

1. V APPC může volající agent MCA označovat ID uživatele, které má být použito pro agenta MCA odezvy. Tomu se říká ID uživatele sítě a vztahuje se pouze na kanály spuštěné jako jednotlivé procesy. Nastavte ID uživatele sítě pomocí parametru USERID definice kanálu.
2. Pokud se nepoužije parametr **USERID** , definice kanálu agenta MCA odezvy může určit jméno uživatele, které musí agent MCA použít. Nastavte ID uživatele pomocí parametru **MCAUSER** v definici kanálu.
3. Pokud nebylo ID uživatele nastaveno žádnou z předchozích (dvou) metod, použije se ID uživatele procesu, který spouští program MCA, nebo ID uživatele nadřazeného procesu (modul listener).

Související pojmy

“Záznamy ověření kanálu” na stránce 47
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

Zabezpečení definic inicializátoru kanálu

Inicializátory inicializátorů kanálu mohou manipulovat pouze členové skupiny mqm.

Inicializátory kanálu produktu IBM MQ nejsou objekty produktu IBM MQ ; přístup k nim není řízen produktem OAM. Produkt IBM MQ neumožňuje uživatelům nebo aplikacím manipulovat s těmito objekty, pokud jejich ID uživatele není členem skupiny mqm. Máte-li aplikaci, která vydá příkaz PCF **StartChannelInitiator**, musí být ID uživatele zadané v deskriptoru zprávy v rámci zprávy PCF členem skupiny mqm na cílovém správci front.

ID uživatele musí být také členem skupiny mqm na cílovém počítači, aby bylo možné vydat ekvivalentní příkazy MQSC pomocí příkazu Escape PCF nebo pomocí příkazu `runmqsc` v nepřímém režimu.

Přenosové fronty

Správci front automaticky umístí vzdálené zprávy do přenosové fronty; pro tuto operaci není vyžadováno žádné speciální oprávnění.

Pokud však potřebujete vložit zprávu přímo do přenosové fronty, vyžaduje to zvláštní oprávnění; viz Tabulka 12 na stránce 127.

Uživatelské procedury kanálu

Nejsou-li záznamy ověření kanálu vhodné, můžete pro přidané zabezpečení použít uživatelské procedury kanálu. Uživatelská procedura zabezpečení vytváří zabezpečené připojení mezi dvěma uživatelskými programy zabezpečení. Jeden program je pro vysílajícího agenta kanálu zpráv (MCA) a jeden je pro přijímajícího agenta MCA.

Další informace o uživatelských procedurách kanálu naleznete v příručce “Ukončovací programy kanálu” na stránce 104 .

Zabezpečení 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 klíčová úložiště

Dobrým zvykem je nastavit atribut návěští certifikátu správce front (**CERTLABL**) na název osobního certifikátu, který má být použit pro většinu kanálů, a přepsat jej pro výjimky tím, že nastavíte jmenovku certifikátu na těchto kanálech, které vyžadují různé certifikáty.

Potřebujete-li mnoho kanálů s certifikáty, které se liší od výchozího nastavení certifikátů ve správci front, měli byste zvážit rozdělení kanálů mezi několik správců front nebo použít server proxy MQIPT před správcem front za účelem předložení jiného certifikátu.

Pro každý kanál můžete použít jiný certifikát, ale pokud ukládáte příliš mnoho certifikátů v úložišti klíčů, můžete očekávat, že bude mít vliv na výkon při spouštění kanálů TLS. Pokuste se zachovat počet certifikátů v úložišti klíčů méně než přibližně 50 a považujte 100 za maximum, protože se výkon sady GSKit výrazně sníží s většími klíčovými úložišti.

Povolení více certifikátů ve stejném správci front zvyšuje pravděpodobnost, že bude ve stejném správci front použito více certifikátů CA. To zvyšuje pravděpodobnost, že obor názvů rozlišujícího názvu certifikátu koliduje s certifikáty vydanými oddělenými certifikačních autorit.

Zatímco profesionální certifikační autority jsou pravděpodobně opatrnější, interní certifikační autority často postrádají jasné konvence pojmenování a vy byste mohli skončit nezamýšlenými shodami mezi CA a jinou CA.

Kromě rozlišujícího názvu subjektu byste měli zkontrolovat rozlišující název vydavatele certifikátu. Chcete-li tak učinit, použijte ověření kanálu SSLPEERMAP a nastavte pole **SSLPEER** i **SSLCERTI** tak, aby se shodovaly s DN subjektu a DN vydávajícího.

Certifikáty podepsané svým držitelem a certifikáty podepsané (CA)

Je důležité naplánovat použití digitálních certifikátů, a to jak při vývoji a testování vaší aplikace, tak i pro její použití při výrobě. V závislosti na použití správců front a klientských aplikací můžete použít certifikáty podepsané CA nebo certifikáty s vlastním podpisem.

Certifikáty podepsané (CA)

V případě produkčních systémů získejte certifikáty od důvěryhodné certifikační autority (CA). Když získáte certifikát od externího CA, zaplatíte za tuto službu.

Certifikáty podepsané svým držitelem

Během vývoje své aplikace můžete používat certifikáty podepsané sebou samým nebo certifikáty vydané lokálním CA v závislosti na platformě:

V systémech AIX, Linux, and Windows můžete používat certifikáty podepsané sebou samým. Pokyny naleznete v příručce “Vytvoření osobního certifikátu podepsaného sebou samým na serveru AIX, Linux, and Windows” na stránce 287.

V systému IBM i můžete používat certifikáty podepsané lokálním CA. Pokyny naleznete v příručce “Požádání o certifikát serveru v systému IBM i” na stránce 272 .

V systému z/OSmůžete použít buď certifikáty podepsané sebou samým, nebo lokální certifikáty podepsané CA. Pokyny naleznete v příručce “Vytvoření osobního certifikátu podepsaného sebou samým na serveru z/OS” na stránce 314 nebo “Požádání o osobní certifikát v systému z/OS” na stránce 315 .

Certifikáty podepsané svým držitelem nejsou vhodné pro provozní účely, a to z těchto důvodů:

- Certifikáty podepsané sebou samým nelze odvolat, což může útočníkovi umožnit, aby po poškození soukromého klíče zanechal totožnost identity. Certifikační úřady mohou odvolat kompromitovaný certifikát, který zabrání jeho dalšímu použití. Certifikáty podepsané certifikační autoritou jsou proto bezpečnější pro použití v produkčním prostředí, ačkoli certifikáty podepsané sebou samým pro testovací systém jsou pohodlnější.
- Platnost certifikátů podepsaných sebou samým nikdy nevyprší. To je výhodné i bezpečné v testovacím prostředí, ale v produkčním prostředí je ponechá otevřené pro případné narušení zabezpečení. Riziko je znásobeno skutečností, že certifikáty podepsané sebou samým nelze odvolat.
- Certifikát s automatickým podpisem se používá jako osobní certifikát i jako kořenový certifikát CA (nebo jeho kotva důvěryhodnosti). Uživatel s osobním certifikátem podepsaným sebou samým by mohl být schopen jej použít k podepisování jiných osobních certifikátů. Obecně platí, že to neplatí pro osobní certifikáty vydané certifikačním úřadem a představují významnou expozici.

CipherSpecs a digitální certifikáty

U všech podporovaných typů digitálních certifikátů lze použít pouze podmnožinu podporovaných CipherSpecs . Je proto nezbytné zvolit příslušnou CipherSpec pro vaše digitální certifikáty. Podobně platí, že pokud vaše zásada zabezpečení vaší organizace vyžaduje použití určité CipherSpec , je třeba získat vhodné digitální certifikáty.

Další informace o vztahu mezi CipherSpecs a digitálními certifikáty viz “Digitální certifikáty a kompatibilita CipherSpec v produktu IBM MQ” na stránce 43

Zásady ověření platnosti certifikátu

Standard IETF RFC 5280 uvádí řadu pravidel pro ověření platnosti certifikátu, které musí implementovat vyhovující aplikační software, aby se zabránilo útokům zosobnění. Sada pravidel pro ověření platnosti certifikátu je známá jako zásada ověření platnosti certifikátu. Další informace o zásadách ověření platnosti certifikátů v produktu IBM MQnaleznete v tématu “Zásady ověření platnosti certifikátu v produktu IBM MQ” na stránce 42.

Plánování kontroly odvolání certifikátů

Povolení více certifikátů z různých certifikačních autorit může potenciálně způsobit zbytečnou další kontrolu odvolání certifikátů.

Konkrétně, pokud jste explicitně nakonfigurovali použití serveru pro odvolání z určité CA, například pomocí objektu AUTHINFO nebo struktury záznamu ověřovacích informací (MQAIR), kontrola odvolání selže, když se předkládá s certifikátem od jiného CA.

Měli byste se vyhnout explicitní konfiguraci serveru odvolaných certifikátů (CRL). Místo toho byste měli povolit implicitní kontrolu, kdy každý certifikát obsahuje vlastní umístění serveru odvolání v rozšíření certifikátu, například v distribučním bodu CRL nebo OCSP AuthorityInfoAccess.

Další informace viz OCSPCheckExtensions a CDPCheckExtensions.

Příkazy a atributy pro podporu TLS

Protokol Transport Layer Security (TLS) poskytuje zabezpečení kanálu, s ochranou proti odposlouchávání, falšování a zosobnění. Podpora produktu IBM MQ pro zabezpečení TLS umožňuje určit v definici kanálu to, že konkrétní kanál používá zabezpečení TLS. Můžete také uvést podrobnosti o typu zabezpečení, jaký chcete, jako například šifrovací algoritmus, který chcete použít.

- Následující příkazy MQSC podporují TLS:

  ZMĚNIT AUTHINFO
  Upraví atributy objektu ověřovacích informací.

  DEFINOVAT AUTHINFO
  Vytvoří objekt ověřovacích informací.

  ODSTRANIT AUTHINFO
  Odstraní objekt ověřovacích informací.

  ZOBRAZIT AUTHINFO
  Zobrazí atributy pro specifický objekt ověřovacích informací.

- Následující parametry správce front podporují TLS:

  CERTLABL
  Definuje jmenovku osobního certifikátu, který má být použit.

  SSLCRLNL
  Atribut SSLCRLNL uvádí seznam názvů objektů ověřovacích informací, které se používají k poskytnutí umístění odvolaných certifikátů k povolení rozšířené kontroly certifikátu TLS.

  SSLCRYP
  V systému AIX, Linux, and Windows nastavuje atribut správce front produktu **SSLCryptoHardware** . Tento atribut je názvem řetězce parametru, který můžete použít ke konfiguraci kryptografického hardwaru, který máte ve vašem systému.

  SSLEV
  Určuje, zda je zpráva o události TLS hlášena v případě, že kanál, který používá TLS, nemůže vytvořit připojení TLS.

  SSLFIPS
  Určuje, zda mají být použity pouze algoritmy certifikované podle standardu FIPS, pokud je šifrování prováděno v produktu IBM MQ , nikoli v kryptografickém hardwaru. Je-li konfigurován kryptografický hardware, jsou použity kryptografické moduly poskytované hardwarovým produktem a tyto šifrovací moduly mohou být certifikovány podle standardu FIPS na konkrétní úroveň. Závisí na tom, který hardware se používá.

  SSLKEYR
  V systémech AIX, Linux, and Windows asociuje úložiště klíčů se správcem front. Databáze klíčů je zadržena v databázi klíčů *GSKit* . Produkt IBM Global Security Kit (GSKit) umožňuje používat zabezpečení TLS v systémech AIX, Linux, and Windows .

  SSLRKEYC
  Počet bajtů, které mají být odeslány a přijaty v rámci konverzace TLS, než je znovu vyjednán tajný klíč. Počet bajtů zahrnuje řídicí informace odeslané agentem MCA.

- Následující parametry kanálu podporují TLS:

  CERTLABL
  Definuje jmenovku osobního certifikátu, který má být použit.

  SSLCAUTH
  Definuje, zda produkt IBM MQ vyžaduje a ověřuje certifikát od klienta TLS.

SSLCIPH
Určuje sílu šifrování a funkci (CipherSpec), například TLS_RSA_WITH_AES_128_CBC_SHA. Shoda CipherSpec musí odpovídat oběma konci kanálu.

SSLPEER
Uvádí rozlišující název (jedinečný identifikátor) povolených partnerů.

Tento oddíl popisuje příkazy **setmqaut**, **dspmqaut**, **dmpmqaut**, **rcrmqobj**, **rcdmqimg**a **dspmqfls** pro podporu objektu ověřovacích informací. Popisuje také 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 části

- “Protokoly zabezpečení TLS v produktu IBM MQ” na stránce 22

Podrobnosti o příkazech MQSC přidružených k protokolu TLS naleznete v

- ALTER AUTHINFO
- Příkaz DEFINE AUTHINFO
- ODSTRANIT AUTHINFO
- ZOBRAZIT AUTHINFO

Podrobnosti o příkazech PCF přidružených k protokolu TLS najdete v tématu

- Změnit, kopírovat a vytvořit objekt ověřovacích informací
- Odstranit objekt ověřovacích informací
- Dotaz na objekt ověřovacích informací

z/OS *IBM MQ for z/OS Kanál připojení serveru*

Kanál SVRCONN produktu IBM MQ for z/OS není zabezpečený bez implementace ověřování kanálu nebo při přidávání uživatelské procedury zabezpečení pomocí protokolu TLS. Kanály SVRCONN nemají při výchozím nastavení zabezpečení definovanou jako výchozí.

Bezpečnostní otázky

Kanály SVRCONN nejsou zabezpečené jako původně definované, SYSTEM.DEF.SVRCONN například. 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 uživatelskou proceduru pro zabezpečení zprávy, napsat uživatelskou proceduru zabezpečení nebo zakoupit uživatelskou proceduru pro zabezpečení zprávy.

K dispozici je několik ukázek, které můžete použít jako dobrý počáteční bod pro zápis vlastního výstupního bodu zabezpečení kanálu SVRCONN.

V produktu IBM MQ for z/OSje člen CSQ4BCX3 ve vaší knihovně hlq.SCSQC37S ukázkou uživatelské procedury zabezpečení napsanou v jazyce C. Ukázka CSQ4BCX3 se také dodává předkompilovaným ve vaší knihovně hlq.SCSQAUTH .

Ukázkovou uživatelskou proceduru CSQ4BCX3 můžete implementovat zkopírováním kompilovaného člena hlq.SCSQAUTH(CSQ4BCX3) do zaváděcí knihovny, která je přidělena k CSQXLIB DD ve vašem CHIN Proc. Všimněte si, že CHIN vyžaduje, aby zaváděcí knihovna byla nastavena jako "Program Controlled".

Upravte kanál SVRCONN, aby nastavil CSQ4BCX3 jako uživatelskou proceduru pro zabezpečení zprávy.

V 9.2.0 Když se klient připojí pomocí daného kanálu SVRCONN, bude produkt CSQ4BCX3 ověřovat pomocí dvojice **RemoteUserIdentifier** a **RemotePassword** z MQCD nebo, z IBM MQ for z/OS 9.1.4, páru **CSPUserIdPtr** a **CSPPasswordPtr** z MQCSP. Je-li ověření úspěšné, zkopíruje **RemoteUserIdentifier** do **MCAUserIdentifier**a změní kontext identity podprocesu.

V případě Long Term Support a Continuous Delivery před IBM MQ for z/OS 9.1.4, když se klient připojí pomocí tohoto kanálu SVRCONN, CSQ4BCX3 provede ověření pomocí páru **RemoteUserIdentifier** a **RemotePassword** z MQCD. Je-li ověření úspěšné, zkopíruje **RemoteUserIdentifier** do **MCAUserIdentifier**a změní kontext identity podprocesu.

Pokud napíšete klienta IBM MQ Java , můžete použít popup k dotazování uživatele a nastavení MQEnvironment.userID a MQEnvironment.password. Tyto hodnoty budou předány při vytvoření připojení.

Nyní, když máte funkční uživatelskou proceduru zabezpečení, existuje další obava, že ID uživatele a heslo jsou přenášeny jako prostý text po síti, když je vytvořeno připojení, stejně jako obsah všech následujících zpráv produktu IBM MQ . TLS můžete použít k šifrování této počáteční informace o připojení a také obsahu všech zpráv produktu IBM MQ .

Příklad

Chcete-li zabezpečit kanál SVRCONN IBM MQ Explorer , 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 knihovna zavedení je Kontrolovaná programem.
3. Upravte SYSTÉM ADMIN.SVRCONN , aby používal proceduru zabezpečení CSQ4BCX3.
4. V produktu IBM MQ Explorerklepněte pravým tlačítkem myši na název správce front produktu z/OS , vyberte volbu **Podrobnosti připojení** > **Vlastnosti** > **ID uživatele** a zadejte ID uživatele produktu z/OS .
5. Připojte se ke správci front produktu z/OS zadáním hesla.

Další informace

Aby bylo možné ukončit program CSQ4BCX3 v prostředí s řízenými programy, vše načtené do adresního prostoru CHIN musí být zavedeno z knihovny řízené programem, například všechny knihovny v knihovně STEPLIB a všechny knihovny pojmenované na CSQXLIB DD. To set a load library as Program Controlled issue RACF commands. V následujícím příkladu je název knihovny načtení MY.TEST.LOADLIB.

```
RALTER PROGRAM * ADDMEM('MY.TEST.LOADLIB'//NOPADCHK)
SETROPTS WHEN(PROGRAM)REFRESH
```

Chcete-li změnit kanál SVRCONN za účelem implementace rozhraní CSQ4BCX3, zadejte následující příkaz IBM MQ :

```
ALTER CHANNEL(SYSTEM ADMIN.SVRCONN) CHLTYPE(SVRCONN) SCYEXIT(CSQ4BCX3)
```

Ve výše uvedeném příkladu se používá název kanálu SVRCONN SYSTEM ADMIN.SVRCONN.

Další informace o uživatelských procedurách kanálu naleznete v příručce “Ukončovací programy kanálu” na stránce 104 .

Související úlohy

Zápis ukončovacích programů kanálu v systému z/OS

Služby zabezpečení architektury SNA LU 6.2

LU technologie SNA 6.2 nabízí šifrování na úrovni relace, ověření na úrovni relace a ověřování na úrovni konverzace.

Poznámka: Tato kolekce témat předpokládá, že máte základní informace o architektuře SNA (Systems Network Architecture). Druhá dokumentace uvedená v tomto oddílu obsahuje stručné úvodní informace o příslušných konceptech a terminologii. Požadujete-li komplexnější technický úvod do SNA, prostudujte si téma *Systems Network Architecture Technical Overview*, GC30-3073.

Logická jednotka SNA 6.2 poskytuje tři bezpečnostní služby:

- Šifrování na úrovni relace
- Ověření úrovně relace
- Ověření úrovně konverzace

V případě šifrování na úrovni relace a ověřování na úrovni relace používá SNA algoritmus *Data Encryption Standard (DES)* . Algoritmus DES je algoritmus šifry bloku, který používá symetrický klíč pro šifrování a dešifrování dat. Oba blok i klíč mají délku 8 bajtů.

Šifrování na úrovni relace
Šifrování na úrovni relace šifruje a dešifruje data relací pomocí algoritmu DES. Lze jej proto použít k zajištění služby utajení na úrovni odkazů na kanálech LU SNA LU 6.2 .

Logické jednotky (LU) mohou poskytovat povinná (nebo požadovaná) šifrování dat, selektivní šifrování dat nebo žádné šifrování dat.

Na *povinném kryptografickém relaci*logická jednotka šifruje všechny odchozí jednotky požadavků na data a dešifruje všechny jednotky příchozích požadavků na data.

Na *výběrové šifrovací relaci*šifruje jednotka LU pouze jednotky dat požadavku zadané odesílajícím transakčním programem (TP). Odesílající LU signalizuje, že data jsou šifrována nastavením indikátoru v záhlaví požadavku. Zaškrtnutím tohoto indikátoru může přijímající logická jednotka zjistit, které jednotky mají být dešifrovány před jejich předáním do přijímajícího transakčního protokolu.

V síti SNA jsou to transakční programy IBM MQ MCAs. MCAs nepožaduje šifrování pro žádná data, která odesílají. Výběrové šifrování dat není proto volbou; v relaci je možné pouze povinné šifrování dat nebo žádné šifrování dat.

Informace o tom, jak implementovat povinné šifrování dat, najdete v dokumentaci k subsystému SNA. Další informace o silnějších formách šifrování, které mohou být k dispozici pro použití na platformě, jako je Triple DES 24bajtové šifrování na serveru z/OS, najdete v příslušné dokumentaci.

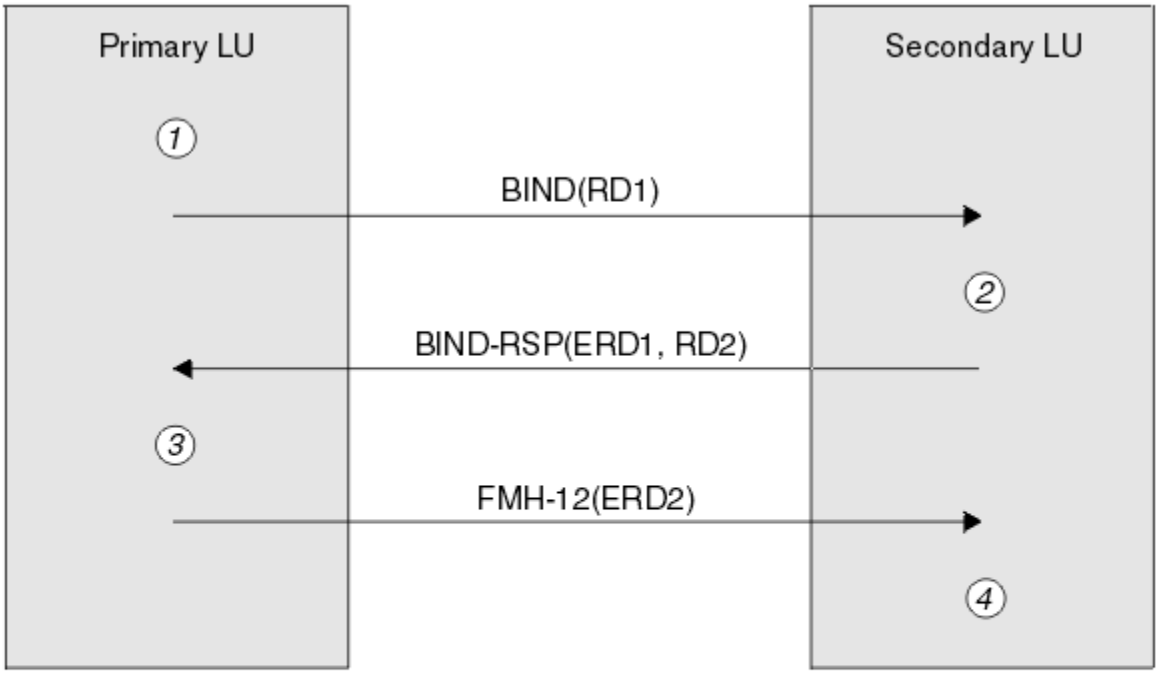
Další obecné informace o šifrování na úrovni relace najdete v tématu *Systems Network Architecture LU 6.2 Reference: Peer Protocols*, SC31-6808.

Ověření úrovně relace
Ověření úrovně relace je protokol zabezpečení na úrovni relace, který umožňuje dvěma jednotkám LU, aby se navzájem ověřovali, zatímco aktivují relaci. Je také známý jako *Verifikace LU-LU*.

Vzhledem k tomu, že logická jednotka je ve skutečnosti "brána" do systému ze sítě, můžete tuto úroveň ověření považovat za dostatečné za určitých okolností. Pokud například správce front potřebuje vyměnit zprávy se vzdáleným správcem front, který je spuštěn v řízeném a důvěryhodném prostředí, můžete být připraveni důvěřovat identitám zbývajících komponent vzdáleného systému po ověření logické jednotky LU.

Ověření úrovně relace je dosaženo každou LU, která ověřuje heslo svého partnera. Heslo se nazývá *heslo LU-LU* , protože jedno heslo se ustanoví mezi každou dvojicí jednotek LU. Způsob, jakým je vytvořeno heslo LU-LU, závisí na implementaci a mimo rozsah SNA.

Obrázek 12 na stránce 116 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 úrovně relace je následující. Čísla v proceduře odpovídají číslům v Obrázek 12 na stránce 116.

1. Primární LU vygeneruje náhodnou datovou hodnotu (RD1) a odešle ji na sekundární LU v požadavku BIND.
2. Když sekundární LU přijme požadavek BIND s náhodnými daty, zašifruje data pomocí algoritmu DES se svou kopií hesla LU-LU jako klíč. Sekundární LU pak vygeneruje druhou náhodnou datovou hodnotu (RD2) a odešle ji s zašifrovanými daty (ERD1) na primární LU v odezvě BIND.
3. Když primární LU obdrží odezvu BIND, vypočítá svou vlastní verzi zašifrovaných dat z náhodných dat, které původně vygenerovala. To lze provést pomocí algoritmu DES a jeho kopií hesla LU-LU jako klíče. Pak porovná svou verzi s zašifrovanými daty, která byla přijata v odezvě BIND. Jsou-li obě hodnoty stejné, primární LU ví, že sekundární LU má stejné heslo, jaké má, a sekundární LU je ověřena. Pokud se tyto dvě hodnoty neshodují, primární LU ukončí relaci.

   Primární jednotka LU pak šifruje náhodná data, která byla přijata v odezvě BIND, a odešle šifrovaná data (ERD2) na sekundární LU v záhlaví správy funkcí 12 (FMH-12).
4. Když sekundární LU přijme FMH-12, vypočítá svou vlastní verzi šifrovaných dat z náhodných dat, která vygenerovala. Pak porovná jeho verzi s zašifrovanými daty, která přijala v FMH-12. Jsou-li tyto dvě hodnoty stejné, je primární LU ověřena. Pokud se tyto dvě hodnoty neshodují, ukončí sekundární LU relaci.

V rozšířené verzi protokolu, která poskytuje lepší ochranu proti muži uprostřed napadení, vypočítá sekundární LU kód DES (Message Authentication Code) DES z RD1, RD2a plně kvalifikovaný název sekundární LU pomocí jeho kopie hesla LU-LU jako klíče. Sekundární LU odesílá MAC primární LU v rámci odezvy BIND místo ERD1.

Primární LU ověřuje sekundární LU pomocí výpočtu své vlastní verze MAC, která porovnává s MAC přijatou v odpovědi BIND. Primární logická jednotka potom vypočítá druhou adresu MAC z RD1 a RD2a místo ERD2odešle adresu MAC na sekundární logickou jednotku v FMH-12 .

Sekundární LU autentizuje primární LU tím, že si vyrovná svou vlastní verzi druhé MAC, která porovná s MAC přijatou v FMH-12.

Informace o tom, jak nakonfigurovat ověření úrovně relace, najdete v dokumentaci k subsystému SNA. Další obecné informace o ověřování na úrovni relace najdete v tématu *Systems Network Architecture LU 6.2 Reference: Peer Protocols*, SC31-6808.

Ověření úrovně konverzace
Když se lokální transakční program pokusí o přidělení konverzace s partnerským transakčním programem, odešle lokální LU operaci připojení k partnerské LU 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 transakčního protokolu. To se označuje jako *ověření na úrovni konverzace*nebo *ověření koncového uživatele*.

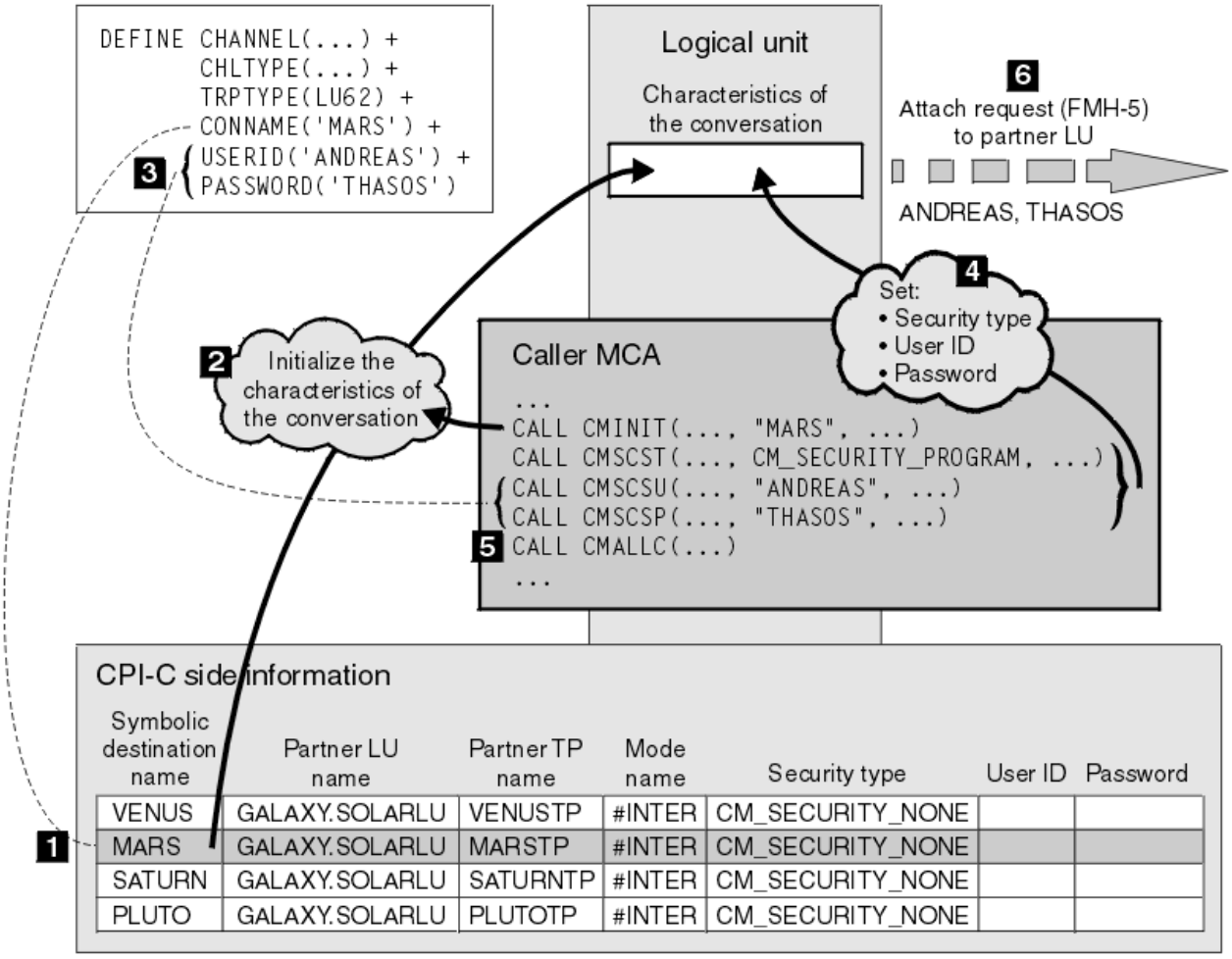
Následující témata popisují, jak produkt IBM MQ poskytuje podporu pro ověření na úrovni konverzace.

Další informace o ověřování na úrovni konverzace najdete v tématu *Systems Network Architecture LU 6.2 Reference: Peer Protocols*, SC31-6808. Informace specifické pro produkt z/OSnaleznete v příručce *z/OS Planning: APPC/MVS Management*, SA22-7599.

Další informace o rozhraní CPI-C naleznete v příručce *Common Programming Interface Communications CPI-C Specification*, SC31-6180. Další informace o službách APPC/MVS CTP Callable Services naleznete v příručce *z/OS MVS Programming: Writing Transaction Programs for APPC/MVS*, SA22-7621.

Multi *Podpora pro ověřování na úrovni konverzace na platformách Multiplatforms*
V tomto tématu získáte přehled o tom, jak funguje ověřování na úrovni konverzace na platformách Multiplatforms.

Podpora pro ověřování na úrovni konverzace u více platforem je ilustrována v tématu Obrázek 13 na stránce 118. Čísla v diagramu odpovídají číslům v níže uvedeném 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 platformách Multiplatform používá agent MCA volání rozhraní CPI-C (Common Programming Interface Communications) pro komunikaci s partnerským agentem MCA v rámci sítě SNA. V definici kanálu na volajícím konci kanálu je hodnota parametru CONNAME symbolickým názvem místa určení, který identifikuje položku informací o připojení CPI-C (1). Tento záznam uvádí:

- Název partnerské LU
- Název partnerského TP, což je agent MCA odezvy.
- Název režimu, který se má použít pro konverzaci

Na straně informační informace lze také zadat následující informace o zabezpečení:

- Typ zabezpečení.

  Běžně implementované typy zabezpečení jsou CM_SECURITY_NONE, CM_SECURITY_PROGRAM a CM_SECURITY_SAME, ale ostatní jsou definováni ve specifikaci CPI-C.
- ID uživatele.
- Heslo.

Volající program MCA se připravuje na přidělení konverzace s agentem MCA pomocí volání CMINIT rozhraní CPI-C s použitím hodnoty CONNAME jako jednoho z parametrů volání. Volání CMINIT identifikuje ve prospěch lokální LU položku informací o připojení, kterou má agent MCA v úmyslu použít pro konverzaci. Lokální LU používá hodnoty v této položce k inicializaci charakteristik konverzace (2).

Volající MCA pak zkontroluje hodnoty parametrů USERID a PASSWORD v definici kanálu (3). Je-li nastaveno USERID, volající agent MCA vydává 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 s hodnotou USERID.
- CMSCSP, abyste nastavili heslo pro konverzaci na hodnotu PASSWORD. CMSCSP se nezavolá, pokud není nastavena hodnota PASSWORD.

Typ zabezpečení, ID uživatele a heslo nastavené těmito voláními přepíší jakékoli hodnoty získané dříve z informací o straně.

Volající MCA pak vydá volání CI-C CMALLC, aby přidělil konverzaci (5). V reakci na toto volání lokální jednotka LU odešle na partnerskou LU (6) požadavek na připojení (záhlaví správy funkcí 5 nebo FMH-5).

Pokud partnerská LU přijme ID uživatele a heslo, hodnoty USERID a PASSWORD jsou zahrnuty v požadavku na připojení. Pokud partnerská LU neakceptuje ID uživatele a heslo, hodnoty nebudou zahrnuty do požadavku na připojení. Lokální LU zjišťuje, zda partnerská LU přijme ID uživatele a heslo jako součást výměny informací, když se relace LU vytvoří pro vytvoření relace.

V novější verzi požadavku na připojení může nahradit heslo mezi jednotkami LU místo jednoznačných hesel. Náhradní heslo je kód DES (Message Authentication Code) DES nebo kód digest zprávy SHA-1 , vytvořený z hesla. Náhražky hesla lze použít pouze v případě, že je podporují obě LU.

Když partnerská LU přijme příchozí požadavek na připojení obsahující ID uživatele a heslo, může pro účely identifikace a ověření použít ID uživatele a heslo. S odkazem na seznamy přístupových práv může partnerská LU také určit, zda má ID uživatele oprávnění k přidělení konverzace a připojení agenta MCA.

Kromě toho může agent MCA být spuštěn pod ID uživatele zahrnutého v požadavku na připojení. V tomto případě se ID uživatele stane výchozím ID uživatele pro modul MCA odezvy a použije se pro kontroly oprávnění, když se agent MCA pokusí připojit ke správci front. Může být také použit pro kontroly oprávnění poté, co 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 váš subsystém SNA najdete v příslušné dokumentaci.

Není-li parametr USERID nastaven, volající agent MCA nezavolá funkce CMSCST, CMSCSU a CMSCSP. V tomto případě jsou informace o zabezpečení, které toky v požadavku na připojení tečou, určeny pouze tím, co je uvedeno v položce informací o straně a jaká partnerská LU bude přijímat.

Ověřování 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/OSMCAs nevyužívá rozhraní CPI-C. Místo toho používají služby APPC/MVS TP Conversation Callable Services, což je implementace programu Advanced Program-to-Program Communication (APPC), která má některé funkce CPI-C. Když volající MCA alokuje konverzaci, je na volání uveden typ zabezpečení STEJNÝ. Vzhledem k tomu, že APPC/MVS LU podporuje trvalé ověření pouze pro příchozí konverzace, ne pro odchozí konverzace, existují dvě možnosti:

- Věří-li partnerská LU APPC/MVS LU a přijme již ověřené ID uživatele, LU APPC/MVS odešle požadavek na připojení obsahující:
  - ID uživatele adresního prostoru inicializátoru kanálu
  - Název profilu zabezpečení, který, je-li použit RACF , je název aktuální skupiny připojení ID uživatele adresního prostoru iniciátoru kanálu
  - Již ověřený indikátor
- Pokud partnerská LU nedůvěřuje LU APPC/MVS a neakceptuje již ověřené ID uživatele, LU APPC/MVS odešle požadavek na připojení neobsahující žádné informace o zabezpečení.

V systému IBM MQ for z/OSnelze parametry USERID a PASSWORD u příkazu DEFINE CHANNEL použít pro kanál zpráv a jsou platné pouze na konci připojení klienta kanálu MQI. Proto požadavek na připojení z APPC/MVS LU nikdy neobsahuje hodnoty zadané těmito parametry.

Zabezpečení klastrů správců front

Ačkoli mohou být klastry správců front vhodné k použití, 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 ke správci front klastru, může být známá ostatním správcům front v klastru. Taková fronta se nazývá *fronta klastru*. Kterýkoli správce front v klastru může odesílat zprávy do front klastru, aniž by bylo nutné některou z následujících položek:

- Explicitní definice vzdálených front pro každou frontu klastru.
- Explicitně definované kanály pro 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.

Odešle-li aplikace připojená ke správci front klastru zprávu do fronty klastru, která má instanci v každém z klonovaných správců front, produkt IBM MQ se rozhodne, kterému správci front má odeslat. Když mnoho aplikací odesílá zprávy do fronty klastru, IBM MQ vyrovnává pracovní zátěž mezi všemi správci front, kteří mají instanci fronty. Dojde-li k selhání jednoho ze systémů, které jsou hostiteli klonovaného správce front, bude produkt IBM MQ i nadále vyrovnávat pracovní zátěž mezi zbývajícími správci front, dokud nebude restartován systém, který selhal.

Používáte-li klastry správců front, je třeba zvážit následující otázky zabezpečení:

- Povolení odesílání zpráv do správce front pouze vybraným správcům front
- Povolení odesílání zpráv do fronty ve správci front pouze vybraným uživatelům vzdáleného správce front
- Povolení aplikací připojených k vašemu správci front pro odesílání zpráv pouze do vybraných vzdálených front

Tyto úvahy jsou relevantní i v případě, že nepoužíváte klastry, ale stávají se důležitějšími, pokud používáte klastry.

Pokud může aplikace odesílat zprávy do jedné fronty klastru, může odesílat zprávy do kterékoli jiné fronty klastru bez potřeby dalších definic vzdálených front, přenosových front nebo kanálů. Proto je důležité zvážit, zda je třeba omezit přístup ke 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 k připojení ke klastru pouze vybraným správcům front
- Vynucení opuštění klastru nechtěným správcům front

Další informace o všech těchto aspektech naleznete v tématu Uchování zabezpečených klastrů.

z/OS Informace o aspektech specifických pro produkt IBM MQ for z/OSnaleznete v tématu “Zabezpečení klastrů správců front v systému z/OS” na stránce 258.

Související úlohy

“Zabránění příjmu zpráv správcem front” na stránce 470
Můžete zabránit správci front klastru, aby přijímal zprávy, které nemá oprávnění přijímat, pomocí ukončovacích programů.

Zabezpečení pro publikování/odběr produktu IBM MQ

Používáte-li produkt IBM MQ Publish/Subscribe, je třeba zvážit další aspekty zabezpečení.

V systému publikování/odběr existují dva typy aplikací: vydavatel a odběratel. *Vydavatelé* poskytují informace ve formě zpráv produktu IBM MQ . Když vydavatel publikuje zprávu, určuje *téma*, které identifikuje předmět informací uvnitř zprávy.

Odběratelé jsou spotřebiteli informací, které jsou publikovány. Odběratel určuje témata, která se zajímají o přihlášení k odběru.

Správce front je aplikace dodávaná s produktem IBM MQ Publish/Subscribe. Obdrží publikované zprávy od vydavatelů a požadavků na odběr od odběratelů a směruje publikované zprávy na odběratele. Odběratel je odeslán pouze na ta témata, k jejichž odběru se přihlásili.

Další informace naleznete v tématu Zabezpečení publikování a odběru.

Zabezpečení výběrového vysílání

Tyto informace vám pomohou pochopit, proč mohou být procesy zabezpečení potřebné pro výběrové vysílání produktu IBM MQ .

Výběrové vysílání produktu IBM MQ nemá vestavěné zabezpečení. Kontroly zabezpečení se zpracovávají ve správci front v době MQOPEN a nastavení pole MQMD je obsluhováno klientem. Některé aplikace v síti nemusí být aplikace IBM MQ (například aplikace LLM, viz Multicast Interoperability with IBM MQ Low Latency Messaging pro více informací), proto byste mohli potřebovat implementovat vaše vlastní procedury zabezpečení, protože přijímající aplikace nemohou být některými z polí kontextu platnosti.

Je třeba zvážit tři procesy zabezpečení:

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 96.

Zabezpečení sítě

Izolovaná síť může být životaschopnou volbou zabezpečení, která zabrání falešným zprávám. Je možné, aby aplikace na adrese skupiny výběrového vysílání publikoval škodlivé zprávy pomocí nativních komunikačních funkcí, které jsou nerozeznatelné od zpráv MQ , protože pocházejí z aplikace na stejné adrese skupinového výběrového vysílání.

Je také možné, aby klient na adrese skupiny výběrového vysílání přijímal zprávy, které byly určeny pro jiné klienty na stejné adrese skupinového výběrového vysílání.

Izolace sítě výběrového vysílání zajišťuje, že přístup mají pouze platní klienti a aplikace. Toto bezpečnostní opatření může zabránit tomu, aby zlovolné zprávy pocházeli z odchozí pošty, a důvěrné informace odcházejí.

Další informace o síťových adresách skupin výběrového vysílání najdete v tématu: Nastavení příslušné sítě pro provoz výběrového vysílání

Digitální podpisy

Digitální podpis je vytvořen šifrováním reprezentace zprávy. Šifrování používá soukromý klíč podepsané osoby a v zájmu efektivity obvykle pracuje na kódu digest zprávy spíše než na samotném zprávě. Digitálně podepsat zprávu před operací MQPUT je dobré bezpečnostní opatření, ale tento proces by mohl mít škodlivé účinky na výkon, pokud existuje velký objem zpráv.

Digitální podpisy se liší tím, že jsou data podepsána. Jsou-li dvě různé zprávy podepsány digitálně stejnou entitou, tyto dva podpisy se liší, ale oba podpisy lze ověřit se stejným veřejným klíčem, tj. veřejným klíčem entity, která podepsala zprávy.

Jak již bylo zmíněno výše v této sekci, může být možné, aby aplikace na adrese skupiny výběrového vysílání publikoval škodlivé zprávy pomocí nativních komunikačních funkcí, které nejsou rozeznatelné od zpráv MQ . Digitální podpisy poskytují důkaz o původu a pouze odesílatel zná soukromý klíč, který poskytuje pádné důkazy o tom, že odesílatel je původcem zprávy.

Další informace o tomto tématu viz “Koncepce šifrování” na stránce 7.

Brány firewall a přímý průchod na Internet

Za normálních okolností byste měli používat ochrannou bariéru (firewall), abyste zabránili přístupu k nepřátelským adresám IP, například při útoku typu DoS (Denial of Service). Možná však budete muset dočasně blokovat adresy IP v rámci IBM MQ, možná i když počkáte na administrátora zabezpečení, aby aktualizoval pravidla brány firewall.

Chcete-li blokovat jednu nebo více adres IP, vytvořte záznam ověřování kanálu typu BLOCKADDR nebo ADDRESSMAP. Další informace viz "Blokování určitých adres IP" na stránce 374.

Zabezpečení pro IBM MQ Internet Pass-Thru

Produkt IBM MQ Internet Pass-Thru může zjednodušit komunikaci prostřednictvím brány firewall, ale má to důsledky zabezpečení.

IBM MQ Internet Pass-Thru (MQIPT) je volitelná komponenta produktu IBM MQ , kterou lze použít k implementaci řešení systému zpráv mezi vzdálenými servery přes internet.

Produkt MQIPT umožňuje dvěma správcům front vyměňovat si zprávy nebo klientskou aplikaci IBM MQ pro připojení ke správci front bez nutnosti přímého připojení TCP/IP. To je užitečné, pokud brána firewall zakazuje přímé připojení TCP/IP mezi dvěma systémy. Proběhne průchod protokolu kanálu produktu IBM MQ a z brány firewall je jednodušší a lépe spravovatelný tunelováním toků uvnitř HTTP nebo serverem jako proxy. Pomocí TLS (Transport Layer Security) lze také používat k šifrování a dešifrování zpráv, které jsou odesílány přes Internet.

Pokud váš systém IBM MQ komunikuje s produktem MQIPT, pokud nepoužíváte režim serveru proxy SSL v produktu MQIPT, ujistěte se, že CipherSpec použitá produktem IBM MQ odpovídá sadě CipherSuite , kterou používá produkt MQIPT:

- Když se produkt MQIPT chová jako server TLS a produkt IBM MQ se připojuje jako klient TLS, musí CipherSpec používaná produktem IBM MQ odpovídat sadě CipherSuite , která je povolena v příslušném svazku klíčů MQIPT .
- Když produkt MQIPT vystupuje jako klient TLS a připojuje se k serveru IBM MQ TLS, musí se MQIPT CipherSuite shodovat s hodnotou CipherSpec definovanou v přijímajícím kanálu IBM MQ .

Provádíte-li migraci z produktu MQIPT na integrovanou podporu protokolu TLS produktu IBM MQ , přeneste digitální certifikáty ze svazku klíčů MQIPT pomocí příkazu **mqiptKeyman** nebo **mqiptKeycmd**.

Další informace viz IBM MQ Internet Pass-Thru.

z/OS Kontrolní seznam implementace zabezpečení produktu IBM MQ for z/OS

Toto téma poskytuje proceduru step-by-step, kterou můžete použít k práci a definování implementace zabezpečení pro každý správce front produktu IBM MQ .

RACF poskytuje definice pro třídy zabezpečení IBM MQ v dodané statické tabulce deskriptoru třídy (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 produktu RACF" na stránce 180.

Podrobnosti naleznete v dalších částech, konkrétně "Profily používané k řízení přístupu k prostředkům produktu IBM MQ" na stránce 189.

Pokud vyžadujete kontrolu zabezpečení, postupujte podle tohoto kontrolního seznamu a implementujte jej:

1. Aktivujte třídu MQADMIN produktu RACF (velké profily) nebo MXADMIN (se smíšenými profily případů).
   - Chcete zabezpečení na úrovni skupiny sdílení front, úroveň správce front nebo kombinaci obojího?

     Viz téma "Profily pro zabezpečení skupiny sdílení front nebo zabezpečení na úrovni správce front" na stránce 185.

2. Potřebujete zabezpečení připojení?
   - **Ano**: Aktivujte třídu MQCONN. Definujte příslušné profily připojení buď 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 CICS nebo IMS ID uživatele adresního prostoru potřebují mít přístup k odpovídajícímu profilu připojení.
   - **Ne**: Definujte hlq.NO.CONNECT.CHECKS profil buď na úrovni správce front, nebo na úrovni skupiny sdílení front ve třídě MQADMIN nebo MXADMIN.
3. Potřebujete kontrolu zabezpečení u příkazů?
   - **Ano**: Aktivujte třídu MQCMDS. Definujte příslušné profily příkazů buď na úrovni správce front, nebo na úrovni skupiny sdílení front ve třídě MQCMDS. Poté povolte příslušným uživatelům nebo skupinám přístup k těmto profilům.

     Pokud používáte skupinu sdílení front, může být nutné zahrnout ID uživatelů používaná samotným správcem front a inicializačním inicialiátorem kanálu. Viz “Nastavení zabezpečení prostředků produktu IBM MQ for z/OS” na stránce 249.
   - **Ne**: Definujte hlq.NO.CMD.CHECKS profil pro požadovaného správce front nebo skupinu sdílení front ve třídě MQADMIN nebo MXADMIN.
4. Potřebujete zabezpečení na prostředcích použitých v příkazech?
   - **Ano**: Ujistěte se, že je třída MQADMIN nebo MXADMIN aktivní. Definujte příslušné profily pro ochranu prostředků u příkazů 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 souboru CSQ6SYSP na výchozí ID uživatele, které má být použito pro kontroly zabezpečení příkazů.

     Pokud používáte skupinu sdílení front, může být nutné zahrnout ID uživatelů používaná samotným správcem front a inicializačním inicialiátorem kanálu. Viz “Nastavení zabezpečení prostředků produktu IBM MQ for z/OS” na stránce 249.
   - **Ne**: Definujte hlq.NO.CMD.RESC.CHECKS profil pro požadovaného správce front nebo skupinu sdílení front ve třídě MQADMIN nebo MXADMIN.
5. Potřebujete zabezpečení fronty?
   - **Ano**: Aktivujte třídu MQQUEUE nebo MXQUEUE. Definujte příslušné profily fronty pro požadovaného správce front nebo skupinu sdílení front ve třídě MQQUEUE nebo MXQUEUEclass. Poté povolte příslušným uživatelům nebo skupinám přístup k těmto profilům.
   - **Ne**: Definujte hlq.NO.QUEUE.CHECKS profil pro požadovaného správce front nebo skupinu sdílení front ve třídě MQADMIN nebo MXADMIN.
6. Potřebujete zabezpečení procesu?
   - **Ano**: Aktivujte třídu MQPROC nebo MXPROC. Definujte příslušné profily procesu na úrovni správce front nebo skupiny sdílení front a povolte těmto profilům přístup k příslušným uživatelům nebo skupinám.
   - **Ne**: Definujte hlq.NO.PROCESS.CHECKS profil pro příslušného správce front nebo skupinu sdílení front ve třídě MQADMIN nebo MXADMIN.
7. Potřebujete zabezpečení seznamu názvů?
   - **Ano**: Aktivace třídy MQNLIST nebo MXNLISTclass. Definujte příslušné profily seznamu názvů na úrovni správce front nebo ve skupině sdílení front ve třídě MQNLIST nebo MXNLIST. Poté povolte příslušným uživatelům nebo skupinám přístup k těmto profilům.
   - **Ne**: Definujte hlq.NO.NLIST.CHECKS profil pro požadovaného správce front nebo skupinu sdílení front ve třídě MQADMIN nebo MXADMIN.
8. Potřebujete zabezpečení témat?

- **Ano**: Aktivujte třídu MXTOPIC. Definujte příslušné profily témat buď 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 hlq.NO.TOPIC.CHECKS profil pro požadovaného správce front nebo skupinu sdílení front ve třídě MQADMIN nebo MXADMIN.

9. Je třeba, aby všichni uživatelé chránili použití voleb MQOPEN nebo MQPUT1 souvisejících s použitím kontextu?
   - **Ano**: Ujistěte se, že je třída MQADMIN nebo MXADMIN 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 hlq.NO.CONTEXT.CHECKS profil pro požadovaného správce front nebo skupinu sdílení front ve třídě MQADMIN nebo MXADMIN.
10. Potřebujete chránit používání alternativních ID uživatelů?
    - **Ano**: Ujistěte se, že je třída MQADMIN nebo MXADMIN aktivní. Definujte příslušnou položku hlq.ALTERNATE.USER. Profily produktu *alternateuserid* pro požadovaného správce front nebo skupiny sdílení front a povolení přístupu vyžadovaných 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 přizpůsobit ID uživatelů, která ID uživatele mají být použita pro kontroly zabezpečení prostředků prostřednictvím RESLEVEL?
    - **Ano**: Ujistěte se, že je třída MQADMIN nebo MXADMIN aktivní. Definujte profil hlq.RESLEVEL buď na úrovni správce front, nebo na úrovni skupiny sdílení front ve třídě MQADMIN nebo MXADMIN. Poté povolte požadovaný přístup uživatelů nebo skupin k profilu.
    - **Ne**: Ujistěte se, že ve třídě MQADMIN nebo MXADMIN neexistují žádné generické profily, které lze použít na hlq.RESLEVEL. Definujte profil hlq.RESLEVEL pro požadovaného správce front nebo skupinu sdílení front a ujistěte se, že k němu nemají přístup žádní uživatelé nebo skupiny.
12. Potřebujete 'timeout' nepoužité ID uživatele z IBM MQ ?
    - **Ano**: Určete hodnoty časového limitu, které byste chtěli použít, a vydejte příkaz MQSC ALTER SECURITY, abyste změnili parametry TIMEOUT a INTERVAL.
    - **Ne**: Vydejte příkaz MQSC ALTER SECURITY, abyste nastavili hodnotu INTERVAL na nulu.

    Poznámka: Aktualizujte vstupní datovou sadu inicializace CSQINP1 používanou vaším podsystémem tak, aby byl příkaz MQSC ALTER SECURITY vydán automaticky při spuštění správce front.
13. Používáte distribuované fronty?
    - **Ano**: Použít záznamy ověření kanálu. Další informace viz téma “Záznamy ověření kanálu” na stránce 47.
    - Můžete také určit příslušnou 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, že každý uživatel, který předloží osobní certifikát TLS obsahující uvedené DN, má použít specifický MCAUSER, nastavte záznam ověřování kanálu typu SSLPEERMAP. Můžete zadat jeden rozlišující název nebo vzorec zahrnující zástupné znaky.
    - Naplánujte infrastrukturu TLS. Nainstalujte funkci System SSL produktu z/OS. V produktu RACFnastavte své filtry názvů certifikátů (CNFs), pokud je používáte, a své digitální certifikáty. Nastavte svazek klíčů SSL. Ujistěte se, že atribut SSLKEYR správce front je neprázdný a ukazuje na váš 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 TLS najdete v tématu “Protokoly zabezpečení TLS v produktu IBM MQ” na stránce 22.

15. Používám klienty?
    - **Ano**: Použít záznamy ověření kanálu.
    - Můžete také určit příslušnou 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 generuje zprávy při spuštění správce front, které zobrazují vaše nastavení zabezpečení. Použijte tyto zprávy k určení, zda jsou vaše přepínače nastaveny správně.
17. Posíláte hesla od klientských aplikací?
    - **Ano**: Ujistěte se, že je nainstalována funkce produktu z/OS a je spuštěna služba Integrated Cryptographic Service Facility (ICSF) pro nejlepší ochranu.
    - **Ne**: Můžete ignorovat chybovou zprávu oznamující, že ICSF není spuštěno.

    Další informace o programu ICSF najdete v tématu "Použití programu ICSF (Integrated Cryptographic Service Facility)" na stránce 258

Nastavení zabezpečení

Tato kolekce témat obsahuje informace specifické pro různé operační systémy a také pro použití klientů.

ALW Nastavení zabezpečení v systému AIX, Linux, and Windows

Aspekty zabezpečení specifické pro systémy AIX, Linux, and Windows .

Správci front produktu IBM MQ přenášejí informace, které jsou potenciálně cenné, a proto je třeba pomocí systému oprávnění zajistit, aby neautorizovaní uživatelé nemohli přistupovat k vašim správcům front. Zvažte následující typy ovládacích prvků zabezpečení:

Kdo může spravovat produkt IBM MQ
Můžete definovat sadu uživatelů, kteří mohou vydávat příkazy pro administraci produktu IBM MQ.

Kdo může používat objekty produktu IBM MQ
Můžete definovat, kteří uživatelé (obvykle aplikace) mohou použít volání MQI a PCF příkazy k provedení následujících úloh:

- Kdo se může připojit ke správci front.
- Kdo může přistupovat k objektům (fronty, definice procesů, seznamy názvů, kanály, kanály připojení klienta, moduly listener, služby a objekty ověřovacích informací) a jaký typ přístupu k těmto objektům mají.
- Kdo má přístup k zprávám produktu IBM MQ .
- Kdo má přístup ke kontextovým informacím přidruženým ke zprávě.

Zabezpečení kanálu
Je třeba zajistit, aby kanály používané k odesílání zpráv na vzdálené systémy měly přístup k požadovaným prostředkům.

Pro udělování přístupu k 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 autorizace k prostředkům MQI.

ALW Jak autorizace fungují na systému AIX, Linux, and Windows

Tabulky specifikací autorizace v tématech v této sekci definují přesně, jak fungují autorizace, a omezení, která se použijí.

Tabulky se vztahují na tyto situace:

- Aplikace, které vydávají volání MQI

- Administrační programy, které vydávají příkazy MQSC jako escape PCF
- Administrační programy, které vydávají příkazy PCF

V této sekci jsou informace prezentována 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, informace o ověření, kanál, kanál připojení klienta, modul listener nebo služba.

Je vyžadována autorizace
Vyjádřeno jako konstanta MQZAO_.

V tabulkách odpovídají v seznamu oprávnění příkazu `setmqaut` pro konkrétní entitu klíčová slova uvedená předponou MQZAO_. Například MQZA_BROWSE odpovídá klíčovému slovu `+browse`, hodnota MQZAO_SET_ALL_CONTEXT odpovídá klíčovému slovu `+setallatd`. Tyto konstanty jsou definovány v souboru záhlaví cmqzc.hdodaném spolu s produktem.

ALW *Oprávnění pro volání MQI*

MQCONN, **MQOPEN**, **MQPUT1**a **MQCLOSE** mohou vyžadovat kontroly autorizace. Tabulky v tomto tématu shrnují autorizace, které jsou zapotřebí pro každé volání.

Aplikace může vydat specifická volání a volby MQI pouze v případě, že je daný identifikátor uživatele, pod kterým je spuštěn (nebo jehož autorizace lze předpokládat), udělena příslušná autorizace.

Čtyři volání MQI mohou vyžadovat kontroly autorizace: **MQCONN**, **MQOPEN**, **MQPUT1**a **MQCLOSE**.

Pro **MQOPEN** a **MQPUT1**je kontrola oprávnění provedena na jménu objektu, který je otevíraný, a nikoli na názvu, nebo názvech, které jsou výsledkem názvu, který byl vyřešen. Například aplikaci může být uděleno oprávnění k otevření fronty alias bez oprávnění k otevření základní fronty, na kterou je alias interpretováno. Pravidlem je, že kontrola se provádí na první definici zjištěné během procesu interpretace názvu, který není alias správce front, pokud definice alias správce front není otevřena přímo; to znamená, že jeho název je zobrazen v poli *ObjectName* deskriptoru objektu. Pro otevíraný objekt je vždy potřeba oprávnění. V některých případech je vyžadováno další oprávnění nezávislé na frontě, získané prostřednictvím autorizace pro objekt správce front.

Tabulka 10 na stránce 126, Tabulka 11 na stránce 127, Tabulka 12 na stránce 127a Tabulka 13 na stránce 128 sumarizují oprávnění potřebná pro každé volání. V tabulkách *Nepoužitelné* znamená, že kontrola autorizace není pro tuto operaci relevantní; *Bez kontroly* znamená, že se neprovádí žádná kontrola autorizace.

Poznámka: V těchto tabulkách nenajdete žádné zmínky o kanálech názvů, kanálech, kanálech připojení klienta, modulech listener, službách nebo objektech ověřovacích informací. Důvodem je to, že se na tyto objekty nevztahují žádná oprávnění, s výjimkou MQOO_INQUIRE, pro které platí stejná oprávnění jako pro ostatní objekty.

Speciální autorizace MQZAO_ALL_MQI obsahuje všechny autorizace v tabulkách, které jsou relevantní pro daný typ objektu, s výjimkou MQZADELETE DELETE a MQZAO_DISPLAY, které jsou klasifikovány jako autorizace pro administraci.

Chcete-li upravit kteroukoli z voleb kontextu zprávy, musíte mít příslušná oprávnění k vydávání volání. Chcete-li například použít funkci MQOO_SET_IDENTITY_CONTEXT nebo MQPMO_SET_IDENTITY_CONTEXT, musíte mít oprávnění `+setid` .

Tabulka 10. Autorizace zabezpečení potřebná pro volání MQCONN

Je vyžadována autorizace pro:	**Objekt fronty (“1” na stránce 128)**	**Objekt procesu**	**Objekt správce front**
MQCONN	Nelze použít	Nelze použít	MQZAO_PŘIPOJENÍ

Tabulka 11. Autorizace zabezpečení potřebná pro volání MQOPEN			
Je vyžadována autorizace pro:	**Objekt fronty (“1” na stránce 128)**	**Objekt procesu**	**Objekt správce front**
MQO_ DOTÁZAT SE	MQZAO_DOTÁZAT SE	MQZAO_DOTÁZAT SE	MQZAO_DOTÁZAT SE
MQOOK_BROWSE	MQZAO_BROWSE	Nelze použít	Žádná kontrola
MQO_INPUT_*	MQZAO_VSTUP	Nelze použít	Žádná kontrola
MQOO_SAVE_ ALL_CONTEXT **(“2” na stránce 128)**	MQZAO_VSTUP	Nelze použít	Nelze použít
MQOO_OUTPUT (normální fronta) **(“3” na stránce 128)**	MQZAO_VÝSTUP	Nelze použít	Nelze použít
MQOO_PASS_ IDENTITY_CONTEXT **(“4” na stránce 128)**	MQZAO_PASS_ IDENTITY_CONTEXT	Nelze použít	Žádná kontrola
MQOO_PASS_ALL_ CONTEXT **(“4” na stránce 128, “5” na stránce 128)**	MQZAO_PASS _ALL_CONTEXT	Nelze použít	Žádná kontrola
MQOO_SET_ IDENTITY_CONTEXT **(“4” na stránce 128, “5” na stránce 128)**	MQZAO_SET_ IDENTITY_CONTEXT	Nelze použít	MQZA_SET_ IDENTITY_CONTEXT **(“6” na stránce 128)**
MQOO_SET_ ALL_CONTEXT **(“4” na stránce 128, “7” na stránce 128)**	MQZAO_SET_ ALL_CONTEXT	Nelze použít	MQZA_SET_ ALL_CONTEXT **(“6” na stránce 128)**
MQOO_OUTPUT (Přenosová fronta) **(“8” na stránce 128)**	MQZAO_SET_ ALL_CONTEXT	Nelze použít	MQZA_SET_ ALL_CONTEXT **(“6” na stránce 128)**
MQOOK_SADA	MQZAO_SADA	Nelze použít	Žádná kontrola
MQO_ALTERNATE_ USER_AUTHORITY	**(“9” na stránce 128)**	**(“9” na stránce 128)**	MQZAO_ALTERNATE_ USER_AUTHORITY **(“9” na stránce 128, “10” na stránce 129)**

Tabulka 12. Autorizace zabezpečení potřebná pro volání MQPUT1			
Je vyžadována autorizace pro:	**Objekt fronty (“1” na stránce 128)**	**Objekt procesu**	**Objekt správce front**
KONTEXT MQPMO_PASS_ IDENTITY_CONTEXT	MQZA_PASS_ IDENTITY_CONTEXT **(“11” na stránce 129)**	Nelze použít	Žádná kontrola
MQPMO_PASS_ALL _CONTEXT	MQZA_PASS_ ALL_CONTEXT **(“11” na stránce 129)**	Nelze použít	Žádná kontrola

Tabulka 12. Autorizace zabezpečení potřebná pro volání MQPUT1 (pokračování)			
Je vyžadována autorizace pro:	**Objekt fronty ("1" na stránce 128)**	**Objekt procesu**	**Objekt správce front**
KONTEXT MQPMO_SET_ IDENTITY_CONTEXT	MQZA_SET_ IDENTITY_CONTEXT **("11" na stránce 129)**	Nelze použít	MQZA_SET_ IDENTITY_CONTEXT **("6" na stránce 128)**
MQPMO_SET_ ALL_CONTEXT	MQZA_SET_ ALL_CONTEXT **("11" na stránce 129)**	Nelze použít	MQZA_SET_ ALL_CONTEXT **("6" na stránce 128)**
(Přenosová fronta) **("8" na stránce 128)**	MQZAO_SET_ ALL_CONTEXT	Nelze použít	MQZA_SET_ ALL_CONTEXT **("6" na stránce 128)**
MQPMO_ALTERNATE_ USER_AUTHORITY	**("12" na stránce 129)**	Nelze použít	MQZAO_ALTERNATE_ USER_AUTHORITY **("10" na stránce 129)**

Tabulka 13. Autorizace zabezpečení potřebná pro volání MQCLOSE			
Je vyžadována autorizace pro:	**Objekt fronty ("1" na stránce 128)**	**Objekt procesu**	**Objekt správce front**
MQCO_DELETE	MQZAO_DELETE **("13" na stránce 129)**	Nelze použít	Nelze použít
VYPRÁZDNIT ODSTRANĚNÍ MQCO_DELETE	MQZAO_DELETE **("13" na stránce 129)**	Nelze použít	Nelze použít

Poznámky k tabulkám:

1. Při otevírání modelové fronty:
   - Pro modelovou frontu je zapotřebí oprávnění MQZAO_DISPLAY, kromě oprávnění k otevření modelové fronty pro typ přístupu, pro který se otevíráte.
   - Oprávnění MQZAO_CREATE není k vytvoření dynamické fronty zapotřebí.
   - Identifikátor uživatele použitý k otevření modelové fronty má automaticky udělena všechna oprávnění specifická pro danou frontu (ekvivalent MQZAO_ALL) pro vytvořenou dynamickou frontu.
2. Musí být zadán také parametr MQOO_INPUT_ *. To platí pro lokální frontu, model nebo alias frontu.
3. Tato kontrola se provádí pro všechny výstupní případy s výjimkou přenosových front (viz poznámka "8" na stránce 128).
4. Musí být zadán také parametr MQOO_OUTPUT.
5. Tuto volbu má také implikovaná hodnota MQO_P_PASS_IDENTITY_CONTEXT.
6. Toto oprávnění je povinné jak pro objekt správce front, tak pro konkrétní frontu.
7. Tato volba předpokládá také MQOO_PASS_IDENTITY_CONTEXT, MQOO_PASS_ALL_CONTEXT a MQOO_SET_IDENTITY_CONTEXT.
8. Tato kontrola se provádí pro lokální nebo modelovou frontu, která má atribut fronty *Usage* MQUS_TRANSMISSION, a je otevírány přímo pro výstup. Nepoužije se, je-li otevřena vzdálená fronta (buď určením názvů vzdáleného správce front a vzdálené fronty, nebo zadáním názvu lokální definice vzdálené fronty).
9. Musí být zadán také alespoň jeden z příkazů MQOO_INQUIRE (pro každý typ objektu) nebo MQOO_BROWSE, MQOO_INPUT_ *, MQOO_OUTPUT nebo MQOO_SET (pro fronty). U provedených kontrol je k dispozici kontrola ostatních voleb s použitím dodaného alternativního identifikátoru

uživatele pro specifické oprávnění k objektu a aktuálního oprávnění aplikace pro kontrolu MQZAALTERNATE_USER_IDENTIFIER.

10. Toto oprávnění umožňuje zadat jakékoli *AlternateUserId* .
11. Kontrola MQZAO_OUTPUT se provádí také tehdy, pokud fronta nemá atribut fronty *Usage* MQUS_TRANSMISION.
12. U provedených kontrol se používají další zadané volby za použití dodaného alternativního identifikátoru uživatele pro konkrétní oprávnění ke frontě a aktuální oprávnění k aplikaci pro kontrolu MQZAALTERNATE_USER_IDENTIFIER.
13. Kontrola se provádí pouze v případě, že jsou splněny obě následující podmínky:
    - Trvalá dynamická fronta se zavírá a odstraňuje.
    - Fronta nebyla vytvořena voláním MQOPEN , které vrátilo použitou obsluhu objektu.

    Jinak žádná kontrola neexistuje.

ALW *Oprávnění pro příkazy MQSC v řídicích PCF*

Tato informace shrnuje oprávnění potřebná pro každý příkaz MQSC, který je obsažen v Escape PCF.

Nepoužije se znamená, že tato operace není pro tento typ objektu relevantní.

ID uživatele, pod kterým je spuštěn program, který spouští příkaz, musí mít také následující oprávnění:

- Oprávnění MQZAO_CONNECT pro správce front
- Oprávnění MQZAO_DISPLAY pro správce front, aby bylo možné provést příkazy PCF
- Oprávnění k vydání příkazu MQSC v textu příkazu Escape PCF

ALTER *objekt*

Objekt	**Je vyžadována autorizace**
Fronta	ZMĚNA MQZAO_CHANGE
Téma	ZMĚNA MQZAO_CHANGE
Proces	ZMĚNA MQZAO_CHANGE
Správce front	ZMĚNA MQZAO_CHANGE
Seznam názvů	ZMĚNA MQZAO_CHANGE
Ověřovací informace	ZMĚNA MQZAO_CHANGE
Kanál	ZMĚNA MQZAO_CHANGE
Kanál připojení klienta	ZMĚNA MQZAO_CHANGE
Modul listener	ZMĚNA MQZAO_CHANGE
Služba	ZMĚNA MQZAO_CHANGE
Informace o komunikaci	ZMĚNA 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

Objekt	Je vyžadována autorizace
Ověřovací informace	Nelze použít
Kanál	Nelze použít
Kanál připojení klienta	Nelze použít
Modul listener	Nelze použít
Služba	Nelze použít
Informace o komunikaci	Nelze použít

DEFINE *objekt* NOREPLACE (“1” na stránce 133)

Objekt	Je vyžadována autorizace
Fronta	MQZAO_CREATE **(“2” na stránce 134)**
Téma	MQZAO_CREATE **(“2” na stránce 134)**
Proces	MQZAO_CREATE **(“2” na stránce 134)**
Správce front	Nelze použít
Seznam názvů	MQZAO_CREATE **(“2” na stránce 134)**
Ověřovací informace	MQZAO_CREATE **(“2” na stránce 134)**
Kanál	MQZAO_CREATE **(“2” na stránce 134)**
Kanál připojení klienta	MQZAO_CREATE **(“2” na stránce 134)**
Modul listener	MQZAO_CREATE **(“2” na stránce 134)**
Služba	MQZAO_CREATE **(“2” na stránce 134)**
Informace o komunikaci	MQZAO_CREATE **(“2” na stránce 134)**

DEFINE *objekt* REPLACE (“1” na stránce 133, “3” na stránce 134)

Objekt	Je vyžadována autorizace
Fronta	ZMĚNA MQZAO_CHANGE
Téma	ZMĚNA MQZAO_CHANGE
Proces	ZMĚNA MQZAO_CHANGE
Správce front	Nelze použít
Seznam názvů	ZMĚNA MQZAO_CHANGE
Ověřovací informace	ZMĚNA MQZAO_CHANGE
Kanál	ZMĚNA MQZAO_CHANGE
Kanál připojení klienta	ZMĚNA MQZAO_CHANGE
Modul listener	ZMĚNA MQZAO_CHANGE
Služba	ZMĚNA MQZAO_CHANGE
Informace o komunikaci	ZMĚNA 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
Služba	MQZAO_DELETE
Informace o komunikaci	MQZAO_DELETE

DISPLAY ***objekt***

Objekt	**Je vyžadována autorizace**
Fronta	MQZAO_ZOBRAZENÍ
Téma	MQZAO_ZOBRAZENÍ
Proces	MQZAO_ZOBRAZENÍ
Správce front	MQZAO_ZOBRAZENÍ
Seznam názvů	MQZAO_ZOBRAZENÍ
Ověřovací informace	MQZAO_ZOBRAZENÍ
Kanál	MQZAO_ZOBRAZENÍ
Kanál připojení klienta	MQZAO_ZOBRAZENÍ
Modul listener	MQZAO_ZOBRAZENÍ
Služba	MQZAO_ZOBRAZENÍ
Informace o komunikaci	MQZAO_ZOBRAZENÍ

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

Objekt	Je vyžadována autorizace
Kanál připojení klienta	Nelze použít
Modul listener	MQZAO_CONTROL
Služba	MQZAO_CONTROL
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
ZMĚNIT DÍLČÍ	Téma	MQZAO_CONTROL
DEFINE SUB	Téma	MQZAO_CONTROL
ODSTRANIT DÍLČÍ	Téma	MQZAO_CONTROL
ZOBRAZIT POD	Téma	MQZAO_ZOBRAZENÍ

Příkazy pro zabezpečení

Příkaz	Objekt	Je vyžadována autorizace
SET AUTHREC	Správce front	ZMĚNA MQZAO_CHANGE
ODSTRANIT AUTHREC	Správce front	ZMĚNA MQZAO_CHANGE
ZOBRAZIT AUTHREC	Správce front	MQZAO_ZOBRAZENÍ

Příkaz	Objekt	Je vyžadována autorizace
ZOBRAZIT AUTHSERV	Správce front	MQZAO_ZOBRAZENÍ
ZOBRAZIT ENTAUTH	Správce front	MQZAO_ZOBRAZENÍ
SET CHLAUTH	Správce front	ZMĚNA MQZAO_CHANGE
ZOBRAZIT VELIKOST CHUSH	Správce front	MQZAO_ZOBRAZENÍ
REFRESH SECURITY	Správce front	ZMĚNA MQZAO_CHANGE

Stavové zobrazení

Příkaz	Objekt	Je vyžadována autorizace
ZOBRAZIT STAV CHSTATUS	Správce front	MQZAO_ZOBRAZENÍ Všimněte si, že v přenosové frontě je vyžadováno oprávnění `+inq` (nebo ekvivalentně MQZAO_INQUIRE), pokud je typ kanálu CLUSSDR.
ZOBRAZIT LSSTATUS	Správce front	MQZAO_ZOBRAZENÍ
ZOBRAZIT PUBSUB	Správce front	MQZAO_ZOBRAZENÍ
ZOBRAZIT STAV SBSTATUS	Správce front	MQZAO_ZOBRAZENÍ
ZOBRAZIT STAV SVSTATUS	Správce front	MQZAO_ZOBRAZENÍ
ZOBRAZIT STAV TPSTATUS	Správce front	MQZAO_ZOBRAZENÍ

Příkazy klastru

Příkaz	Objekt	Je vyžadována autorizace
ZOBRAZIT CLUQMGR	Správce front	MQZAO_ZOBRAZENÍ
Aktualizovat klastr	Vyžadováno členství ve skupině 'mqm'	
Reset klastru	Vyžadováno členství ve skupině 'mqm'	
SUSPEND QMgr	Vyžadováno členství ve skupině 'mqm'	
OBNOVIT SPRÁVCE FRONT	Vyžadováno členství ve skupině 'mqm'	

Další administrativní příkazy

Příkaz	Objekt	Je vyžadována autorizace
ODESLÁNÍ PŘÍKAZU PING	Správce front	MQZAO_ZOBRAZENÍ
AKTUALIZOVAT SPRÁVCE FRONT	Správce front	ZMĚNA MQZAO_CHANGE
RESETOVAT QMGR	Správce front	ZMĚNA MQZAO_CHANGE
ZOBRAZIT PŘIPOJENÍ	Správce front	MQZAO_ZOBRAZENÍ
ZASTAVIT PŘIPOJENÍ	Správce front	ZMĚNA MQZAO_CHANGE

Poznámka:

1. Pro příkazy DEFINE je pro objekt LIKE také zapotřebí oprávnění MQZAO_DISPLAY, je-li zadán, nebo na příslušném SYSTEM.DEFAULT.xxx , je-li LIKE vynechán.

2. Oprávnění CREATE MQZAO_CREATE není specifické pro konkrétní objekt nebo typ objektu. Oprávnění k vytvoření je uděleno pro všechny objekty pro určitého správce front uvedením typu objektu QMGR v příkazu `setmqaut` .
3. To platí, pokud objekt, který má být nahrazen, již existuje. Pokud tomu tak není, kontrola je určena pro atribut DEFINE *object* NOREPLACE.

Související informace

Klastrování: Využití doporučených postupů pro příkaz REFRESH CLUSTER

ALW *Oprávnění pro příkazy PCF*

Tato sekce shrnuje oprávnění potřebná pro každý příkaz PCF.

Žádná kontrola znamená, že není prováděna žádná kontrola autorizace; *Nepoužije se* znamená, že tato operace není pro tento typ objektu relevantní.

ID uživatele, pod kterým je spuštěn program, který spouští příkaz, musí mít také následující oprávnění:

- Oprávnění MQZAO_CONNECT pro správce front
- Oprávnění MQZAO_DISPLAY pro správce front, aby bylo možné provést příkazy PCF

Speciální autorizace MQZAO_ALL_ADMIN zahrnuje všechny autorizace v následujícím seznamu, které jsou relevantní pro daný typ objektu, s výjimkou MQZAO_CREATE, který není specifický pro konkrétní objekt nebo typ objektu.

Změna *objektu*

Objekt	**Je vyžadována autorizace**
Fronta	ZMĚNA MQZAO_CHANGE
Téma	ZMĚNA MQZAO_CHANGE
Proces	ZMĚNA MQZAO_CHANGE
správce front	ZMĚNA MQZAO_CHANGE
Seznam názvů	ZMĚNA MQZAO_CHANGE
Ověřovací informace	ZMĚNA MQZAO_CHANGE
Kanál	ZMĚNA MQZAO_CHANGE
Kanál připojení klienta	ZMĚNA MQZAO_CHANGE
Modul listener	ZMĚNA MQZAO_CHANGE
Služba	ZMĚNA MQZAO_CHANGE
Informace o komunikaci	ZMĚNA 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

Objekt	Je vyžadována autorizace
Kanál připojení klienta	Nelze použít
Modul listener	Nelze použít
Služba	Nelze použít
Informace o komunikaci	Nelze použít

Kopírování *objektu* (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 140)**

Kopírování *objektu* (s nahrazením) (1, 4)

Objekt	Je vyžadována autorizace
Fronta	ZMĚNA MQZAO_CHANGE
Téma	ZMĚNA MQZAO_CHANGE
Proces	ZMĚNA MQZAO_CHANGE
Správce front	Nelze použít
Seznam názvů	ZMĚNA MQZAO_CHANGE
Ověřovací informace	ZMĚNA MQZAO_CHANGE
Kanál	ZMĚNA MQZAO_CHANGE
Kanál připojení klienta	ZMĚNA MQZAO_CHANGE
Modul listener	ZMĚNA MQZAO_CHANGE
Služba	ZMĚNA MQZAO_CHANGE
Informace o komunikaci	ZMĚNA MQZAO_CHANGE

Vytvořit *objekt* (bez náhrady) (3)

Objekt	Je vyžadována autorizace
Fronta	MQZAO_CREATE **(2)**
Téma	MQZAO_CREATE **(2)**

Objekt	Je vyžadována autorizace
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)**

Vytvořit *objekt* (s nahrazením) (3, 4)

Objekt	Je vyžadována autorizace
Fronta	ZMĚNA MQZAO_CHANGE
Téma	ZMĚNA MQZAO_CHANGE
Proces	ZMĚNA MQZAO_CHANGE
Správce front	Nelze použít
Seznam názvů	ZMĚNA MQZAO_CHANGE
Ověřovací informace	ZMĚNA MQZAO_CHANGE
Kanál	ZMĚNA MQZAO_CHANGE
Kanál připojení klienta	ZMĚNA MQZAO_CHANGE
Modul listener	ZMĚNA MQZAO_CHANGE
Služba	ZMĚNA MQZAO_CHANGE
Informace o komunikaci	ZMĚNA 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

Objekt	Je vyžadována autorizace
Informace o komunikaci	MQZAO_DELETE

Zjišťovat *objekt*

Objekt	Je vyžadována autorizace
Fronta	MQZAO_ZOBRAZENÍ
Téma	MQZAO_ZOBRAZENÍ
Proces	MQZAO_ZOBRAZENÍ
správce front	MQZAO_ZOBRAZENÍ
Seznam názvů	MQZAO_ZOBRAZENÍ
Ověřovací informace	MQZAO_ZOBRAZENÍ
Kanál	MQZAO_ZOBRAZENÍ
Kanál připojení klienta	MQZAO_ZOBRAZENÍ
Modul listener	MQZAO_ZOBRAZENÍ
Služba	MQZAO_ZOBRAZENÍ
Informace o komunikaci	MQZAO_ZOBRAZENÍ

Zjišťovat názvy *objektů*

Objekt	Je vyžadována autorizace
Fronta	Žádná kontrola
Téma	Žádná kontrola
Proces	Žádná kontrola
Správce front	Žádná kontrola
Seznam názvů	Žádná kontrola
Ověřovací informace	Žádná kontrola
Kanál	Žádná kontrola
Kanál připojení klienta	Žádná kontrola
Modul listener	Žádná kontrola
Služba	Žádná kontrola
Informace o komunikaci	Žádná kontrola

Spustit *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
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_ZOBRAZENÍ

Příkazy pro zabezpečení

Příkaz	Objekt	Je vyžadována autorizace
Nastavit záznam oprávnění	Správce front	ZMĚNA MQZAO_CHANGE

Příkaz	Objekt	Je vyžadována autorizace
Odstranit záznam oprávnění	Správce front	ZMĚNA MQZAO_CHANGE
Zjistit záznamy oprávnění	Správce front	MQZAO_ZOBRAZENÍ
Zjistit službu ověřování oprávnění	Správce front	MQZAO_ZOBRAZENÍ
Zjišťovat oprávnění pro entitu	Správce front	MQZAO_ZOBRAZENÍ
Nastavit záznam ověření kanálu	Správce front	ZMĚNA MQZAO_CHANGE
Zjistit záznam ověření kanálu	Správce front	MQZAO_ZOBRAZENÍ
Aktualizovat zabezpečení	Správce front	ZMĚNA MQZAO_CHANGE

Stavové zobrazení

Příkaz	Objekt	Je vyžadována autorizace
Zjistit stav kanálu	Správce front	MQZAO_ZOBRAZENÍ Všimněte si, že v přenosové frontě je vyžadováno oprávnění `+inq` (nebo ekvivalentně MQZAO_INQUIRE), pokud je typ kanálu CLUSSDR.
Dotaz na stav modulu listener kanálu	Správce front	MQZAO_ZOBRAZENÍ
Dotaz na stav publikování/odběru	Správce front	MQZAO_ZOBRAZENÍ
Dotaz na stav odběru	Správce front	MQZAO_ZOBRAZENÍ
Zjistit stav služby	Správce front	MQZAO_ZOBRAZENÍ
Zjistit stav tématu	Správce front	MQZAO_ZOBRAZENÍ

Příkazy klastru

Příkaz	Objekt	Je vyžadována autorizace
Zjistit správce front klastru	Správce front	MQZAO_ZOBRAZENÍ
Aktualizovat klastr	Vyžadováno členství ve skupině 'mqm'	Vyžadováno členství ve skupině 'mqm'
Reset klastru	Vyžadováno členství ve skupině 'mqm'	Vyžadováno členství ve skupině 'mqm'
Pozastavit klastr správců front	Vyžadováno členství ve skupině 'mqm'	Vyžadováno členství ve skupině 'mqm'
Obnovit klastr správců front	Vyžadováno členství ve skupině 'mqm'	Vyžadováno členství ve skupině 'mqm'

Další administrativní příkazy

Příkaz	Objekt	Je vyžadována autorizace
Odeslat signál Ping pro správce front	Správce front	MQZAO_ZOBRAZENÍ

Příkaz	Objekt	Je vyžadována autorizace
Aktualizovat správce front	Správce front	ZMĚNA MQZAO_CHANGE
Obnovit správce front	Správce front	ZMĚNA MQZAO_CHANGE
Obnovit statistiku front	Fronta	Funkce MQZAO_DISPLAY a MQZAO_CHANGE
Zjistit připojení	Správce front	MQZAO_ZOBRAZENÍ
Zastavit připojení	Správce front	ZMĚNA MQZAO_CHANGE

Poznámka:

1. Pro příkazy Kopírovat je oprávnění MQZAO_DISPLAY také potřebné pro objekt From.
2. Oprávnění CREATE MQZAO_CREATE není specifické pro konkrétní objekt nebo typ objektu. Oprávnění k vytvoření je uděleno pro všechny objekty pro určitého správce front uvedením typu objektu QMGR v příkazu `setmqaut` .
3. Pro příkazy Create je zapotřebí oprávnění MQZAO_DISPLAY také pro příslušný SYSTEM.DEFAULT.* objekt.
4. To platí, pokud objekt, který má být nahrazen, již existuje. Pokud tomu tak není, je kontrola funkce Kopírovat nebo Vytvořit bez náhrady.

AIX Vytvoření a správa skupin v systému AIX

V systému AIX, pokud nepoužíváte NIS nebo NIS +, použijte SMITTY pro práci se skupinami.

Informace o této úloze

V systému AIXmůžete použít SMITTY k vytvoření skupiny, přidání uživatele do skupiny, zobrazení seznamu uživatelů, kteří jsou ve skupině, a k odstranění uživatele ze skupiny.

Postup

1. Ze souboru SMITTY vyberte volbu **Zabezpečení a uživatelé** a stiskněte klávesu Enter.
2. Vyberte **Skupiny** a stiskněte klávesu Enter.
3. Chcete-li vytvořit skupinu, proveďte následující kroky:
   a) Vyberte volbu **Přidat skupinu** a stiskněte klávesu Enter.
   b) Zadejte název skupiny a názvy všech uživatelů, které chcete přidat do skupiny, a oddělte je čárkami.
   c) Chcete-li vytvořit skupinu, stiskněte klávesu Enter.
4. Chcete-li přidat uživatele do skupiny, proveďte následující kroky:
   a) Vyberte volbu **Změnit/Zobrazit vlastnosti skupin** a stiskněte klávesu Enter.
   b) Zadejte název skupiny, abyste zobrazili seznam členů skupiny.
   c) Přidejte jména uživatelů, které chcete přidat do skupiny, a oddělte je čárkami.
   d) Stisknutím klávesy Enter přidejte jména do skupiny.
5. Chcete-li zobrazit uživatele ve skupině, postupujte podle následujících kroků:
   a) Vyberte volbu **Změnit/Zobrazit vlastnosti skupin** a stiskněte klávesu Enter.
   b) Zadejte název skupiny, abyste zobrazili seznam členů skupiny.
6. Chcete-li odebrat uživatele ze skupiny, postupujte takto:
   a) Vyberte volbu **Změnit/Zobrazit vlastnosti skupin** a stiskněte klávesu Enter.
   b) Zadejte název skupiny, abyste zobrazili seznam členů skupiny.
   c) Odstraňte jméno uživatele, kterého chcete odstranit ze skupiny.

d) Chcete-li název odebrat ze skupiny, stiskněte klávesu Enter.

Linux Vytvoření a správa skupin v systému Linux

V systému Linuxza předpokladu, že nepoužíváte NIS nebo NIS +, použijte soubor `/etc/group` pro práci se skupinami.

Informace o této úloze

V systému Linuxse informace o skupině nacházejí v souboru `/etc/group` . Můžete použít příkazy k vytvoření skupiny, přidání uživatele do skupiny, zobrazení seznamu 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 *ID-skupiny* je číselný identifikátor skupiny a *název-skupiny* je název skupiny.
2. Chcete-li přidat člena do doplňkové skupiny, použijte příkaz **usermod** k vypsání seznamu doplňkových skupin, kterých je uživatel momentálně členem, a doplňkových skupin, kterých se má uživatel stát členem.
   Pokud je například uživatel již členem skupiny `groupa`a stane se členem produktu `groupb`, použijte tento příkaz:
   ```
   usermod -G groupa,groupb user-name
   ```
   kde *jméno-uživatele* je jméno uživatele.
3. Chcete-li zobrazit uživatele, který 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, použijte příkaz **usermod** k vypsání seznamu doplňkových skupin, do kterých má uživatel zůstat členem.
   Je-li například primární skupina uživatele `users` a uživatel je také členem skupin `mqm`, `groupa` a `groupb`, abyste odebrali uživatele ze skupiny `mqm` , použijte tento příkaz:
   ```
   usermod -G groupa,groupb user-name
   ```
   kde *jméno-uživatele* je jméno uživatele.

Windows Vytvoření a správa skupin v systému Windows

V systému Windowspoužíváte funkci Správa počítače k administraci skupin na počítači pracovní stanice nebo na počítači s členskými servery.

Informace o této úloze

Pro řadiče domény jsou uživatelé a skupiny spravovány prostřednictvím Active Directory. Další podrobnosti o použití volby Active Directory najdete v příslušných pokynech k operačnímu systému.

Jakékoli změny, které provedete v členství ve skupině činitele, nebudou rozpoznány, dokud nebude správce front restartován, nebo pokud zadáte příkaz MQSC **REFRESH SECURITY** (nebo ekvivalent PCF).

Použijte panel Správa počítače Windows pro práci s uživateli a skupinami. Jakékoli změny provedené u aktuálně přihlášeného uživatele nemusí být účinné, dokud se uživatel znovu nepřihlásí.

Windows *Vytvoření skupiny v systému Windows*

Vytvořte skupinu pomocí ovládacího panelu.

Postup

1. Otevřete ovládací panel
2. Poklepejte na **Administrativní nástroje**.
   Otevře se panel Administrativní nástroje.
3. Dvakrát klepněte na volbu **Správa počítače**.
   Otevře se panel Správa počítačů.
4. Rozbalte volbu **Lokální uživatelé a skupiny**.
5. Klepněte pravým tlačítkem myši na **Skupiny**a vyberte **Nová skupina ...**.
   Zobrazí se panel Nová skupina.
6. Do pole Název skupiny zadejte odpovídající název a poté klepněte na tlačítko **Vytvořit**.
7. Klepněte na **Zavřít**.

Windows *Přidání uživatele do skupiny v systému Windows*

Přidejte uživatele do skupiny pomocí ovládacího panelu.

Postup

1. Otevřete ovládací panel
2. Poklepejte na **Administrativní nástroje**.
   Otevře se panel Administrativní nástroje.
3. Dvakrát klepněte na volbu **Správa počítače**.
   Otevře se panel Správa počítačů.
4. V panelu Správa počítačů rozbalte **Lokální uživatelé a skupiny**.
5. Vyberte volbu **Uživatelé** .
6. Dvakrát klepněte na uživatele, kterého chcete přidat do skupiny.
   Zobrazí se panel vlastností uživatele.
7. Vyberte kartu **Člen skupiny** .
8. Vyberte skupinu, do které chcete přidat uživatele. Pokud není skupina, kterou chcete zobrazit, viditelná:
   a) Klepněte na tlačítko **Přidat**.
      Zobrazí se panel Výběr skupin.
   b) Klepněte na volbu **Lokality ...**.
      Zobrazí se panel Lokality.
   c) Vyberte umístění skupiny, do které chcete přidat uživatele ze seznamu, a klepněte na tlačítko **OK**.
   d) Do poskytnutého pole zadejte název skupiny.

      Případně klepněte na volbu **Rozšířené ...** a pak **Vyhledat nyní** , abyste vypsali skupiny, které jsou k dispozici v aktuálně vybraném umístění. Ze seznamu vyberte skupinu, do které chcete uživatele přidat, a klepněte na tlačítko **OK**.
   e) Klepněte na tlačítko **OK**.
      Zobrazí se panel vlastností uživatele se zobrazením skupiny, kterou jste přidali.
   f) Vyberte skupinu.
9. Klepněte na tlačítko **OK**.

Zobrazí se panel Správa počítače.

Windows *Zobrazení uživatele ve skupině v systému Windows*

Zobrazit členy skupiny pomocí ovládacího panelu.

Postup

1. Otevřete ovládací panel
2. Poklepejte na **Administrativní nástroje**.
   Otevře se panel Administrativní nástroje.
3. Dvakrát klepněte na volbu **Správa počítače**.
   Otevře se panel Správa počítačů.
4. V panelu Správa počítačů rozbalte **Lokální 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*

Odebrat uživatele ze skupiny pomocí ovládacího panelu.

Postup

1. Otevřete ovládací panel
2. Poklepejte na **Administrativní nástroje**.
   Otevře se panel Administrativní nástroje.
3. Dvakrát klepněte na volbu **Správa počítače**.
   Otevře se panel Správa počítačů.
4. V panelu Správa počítačů rozbalte **Lokální uživatelé a skupiny**.
5. Vyberte volbu **Users** (Uživatelé).
6. Dvakrát klepněte na uživatele, kterého chcete přidat do skupiny.
   Zobrazí se panel vlastností uživatele.
7. Vyberte kartu **Člen skupiny** .
8. Vyberte skupinu, ze které chcete uživatele odebrat, a poté 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 v systému Windows

Některé funkce zabezpečení se chovají různě v různých verzích produktu Windows.

Zabezpečení produktu IBM MQ spoléhá na volání rozhraní API operačního systému na informace o autorizacích uživatele a členství ve skupinách. Některé funkce se v systémech Windows chovají stejně. Tato kolekce témat zahrnuje popisy toho, jak mohou tyto rozdíly ovlivnit zabezpečení produktu IBM MQ , když spouštíte produkt IBM MQ v prostředí produktu 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 každém uživateli, který se o takový přístup pokouší.

- "Konfigurace speciálních uživatelských účtů s produktem Prepare IBM MQ Wizard" na stránce 144
- "Použití IBM MQ s Active Directory" na stránce 144
- "Uživatelská práva vyžadovaná pro službu IBM MQ Windows Service" na stránce 145

Konfigurace speciálních uživatelských účtů s produktem Prepare IBM MQ Wizard

Produkt Prepare IBM MQ Wizard vytvoří speciální uživatelský účet, aby služba Windows mohla sdílet procesy, které je potřebují používat (viz Konfigurace produktu IBM MQ s PPrepare IBM MQ Wizard).

Služba Windows je sdílena mezi klientskými procesy pro instalaci produktu IBM MQ . Pro každou instalaci se vytvoří jedna služba. Každá služba má název `MQ_`*`InstallationName`* a má zobrazovaný název `IBM MQ(`*`InstallationName`*`)`.

Vzhledem k tomu, že každá služba musí být sdílena mezi neinteraktivními a interaktivními relacemi přihlášení, musíte je spustit pod zvláštním uživatelským účtem. Pro všechny služby můžete použít jeden speciální uživatelský účet, nebo můžete vytvořit různé speciální uživatelské účty. Každý speciální uživatelský účet musí mít právo uživatele na `Přihlásit se jako služba`, abyste získali další informace, viz Tabulka 14 na stránce 145. Pokud ID uživatele nemá oprávnění ke spuštění služby, služba se nespustí a vrátí chybu v protokolu událostí systému Windows . Zpravidla se spustí Prepare IBM MQ Wizarda nastaví se ID uživatele správně. Pokud jste však ID uživatele nakonfigurovali ručně, je možné, že budete mít problém, který je třeba vyřešit.

Když instalujete produkt IBM MQ a poprvé spustíte produkt Prepare IBM MQ Wizard , vytvoří lokální uživatelský účet pro službu s názvem MUSR_MQADMIN s požadovanými nastaveními a oprávněními, včetně volby `Logon as a service`.

Pro následné instalace vytvoří produkt Prepare IBM MQ Wizard 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, když se vytvoří účet, a použije se ke konfiguraci přihlašovacího prostředí pro službu. Vygenerované heslo nevyprší.

Tento účet IBM MQ není ovlivněn žádnými zásadami účtu, které jsou nastaveny na systému tak, aby požadovaly, aby byla hesla účtu změněna po určité době.

Heslo není známé mimo toto jednorázové zpracování a je uloženo pomocí operačního systému Windows v zabezpečené části registru.

Použití IBM MQ s Active Directory

V některých konfiguracích sítě, kde jsou uživatelské účty definovány na řadičích domény, které používají adresářovou službu Active Directory , lokální uživatelský účet, pod kterým je portál IBM MQ spuštěn, nemusí mít oprávnění, které vyžaduje k dotazování na členství ve skupinách ostatních uživatelských účtů domény. Při instalaci produktu IBM MQidentifikuje produkt Prepare IBM MQ Wizard informaci o tom, zda se jedná o tento případ, tím, že provedete testy a položíte dotazy na konfiguraci sítě.

Pokud účet lokálního uživatele, pod kterým běží IBM MQ , nemá požadované oprávnění, vyzve vás Prepare IBM MQ Wizard k zadání podrobností o účtu uživatele domény s konkrétními uživatelskými právy. Informace o tom, jak vytvořit a nastavit doménový účet domény Windows , najdete 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 145.

Když jste zadali platné podrobnosti o účtu pro uživatelský účet domény do produktu Prepare IBM MQ Wizard, nakonfiguruje průvodce službu IBM MQ Windows , aby se spustila pod novým účtem. Podrobnosti o účtu jsou zadrženy v zabezpečené části registru a uživatelé jej nemohou číst.

Když je služba spuštěna, služba IBM MQ Windows se spustí a zůstane spuštěná tak dlouho, jak je služba spuštěna. Administrátor produktu IBM MQ , který se přihlásí na server po spuštění služby Windows , může pomocí produktu IBM MQ Explorer spravovat správce front na serveru. Tím se připojí IBM MQ Explorer 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 vyžadovaná pro lokální účty a uživatelské účty domény, pod kterými je spuštěna služba Windows pro instalaci produktu IBM MQ .

Tabulka 14. Uživatelská práva vyžadovaná pro službu systému IBM MQ Windows

Oprávnění	**Popis**
Přihlašovat se jako dávková úloha	Umožňuje spuštění služby IBM MQ Windows pod tímto uživatelským účtem.
Přihlásit jako služba.	Umožňuje uživatelům nastavit službu IBM MQ Windows tak, aby se přihlašuje pomocí konfigurovaného účtu.
Ukončit běh systému	Umožňuje službě IBM MQ Windows restartovat server, je-li konfigurován tak, aby došlo k selhání při obnově služby.
Zvýšit kvóty	Nezbytné pro volání operačního systému `CreateProcessAsUser` .
Vystupovat jako část operačního systému	Nezbytné pro volání operačního systému `LogonUser` .
Obejít kontrolu procházení	Nezbytné pro volání operačního systému `LogonUser` .
Zaměnit úroveň procesu	Nezbytné pro volání operačního systému `LogonUser` .

Poznámka: Práva na ladění programů mohou být zapotřebí v prostředích, kde jsou spuštěny aplikace ASP a IIS.

Uživatelský účet vaší domény musí mít tato uživatelská práva Windows nastavená jako účinná uživatelská práva, která jsou uvedena v aplikaci Lokální zásada zabezpečení. Pokud nejsou, nastavte je buď pomocí lokální aplikace zásad zabezpečení lokálně na serveru, nebo pomocí domény Aplikace zabezpečení domény v široké části.

Windows *Oprávnění zabezpečení serveru Windows*

Instalace produktu IBM MQ se chová jinak na serveru Windows , v závislosti na tom, zda lokální uživatel nebo uživatel domény provádí instalaci.

Pokud *lokální* uživatel nainstaluje produkt IBM MQ, produkt Prepare IBM MQ Wizard zjistí, že lokální uživatel vytvořený pro službu IBM MQ Windows může načíst informace o členství ve skupině pro uživatele instalace. Produkt Prepare IBM MQ Wizard požádá uživatele o otázky o konfiguraci sítě, aby určil, zda jsou definovány jiné uživatelské účty na řadičích domény spuštěných v systému Windows 2000 nebo novějším. Je-li tomu tak, služba IBM MQ Windows musí být spuštěna pod uživatelským účtem domény s konkrétním nastavením a oprávněními. Produkt Prepare IBM MQ Wizard vyzve uživatele k zadání podrobností o účtu tohoto uživatele, jak je popsáno v tématu Konfigurace produktu IBM MQ s produktem Prepare IBM MQ Wizard.

Pokud uživatel *doména* instaluje produkt IBM MQ, produkt Prepare IBM MQ Wizard zjistí, že lokální uživatel vytvořený pro službu IBM MQ Windows nemůže načíst informace o členství ve skupině pro uživatele s instalací. V takovém případě portál Prepare IBM MQ Wizard vždy vyzve uživatele k zadání podrobností o účtu domény uživatele domény, které má služba IBM MQ Windows použít.

Když služba IBM MQ Windows potřebuje použít uživatelský účet domény, IBM MQ nemůže správně fungovat, dokud nebude tento účet nakonfigurován pomocí Prepare IBM MQ Wizard. Produkt Prepare IBM MQ Wizard neumožňuje uživateli pokračovat s jinými úlohami, dokud nebude služba Windows konfigurována s vhodným účtem.

Další informace naleznete v tématu Vytvoření a nastavení doménových účtů pro produkt IBM MQ.

Windows *Změna jména uživatele přidruženého ke službě IBM MQ*

Jméno uživatele přidružené ke službě IBM MQ můžete změnit tak, že vytvoříte nový účet a zadáte jeho podrobnosti pomocí Prepare IBM MQ Wizard.

Informace o této úloze

Když instalujete produkt IBM MQ a poprvé spustíte produkt Prepare IBM MQ Wizard , vytvoří lokální uživatelský účet pro službu s názvem MUSR_MQADMIN. Pro následné instalace vytvoří produkt Prepare IBM MQ Wizard 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. Pokud je například správce front asociován s produktem Db2, který nepřijímá jména uživatelů s více než 8 znaky, může být nutné tuto akci provést.

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 s produktem Prepare IBM MQ Wizard

Windows *Změna hesla lokálního uživatelského účtu služby IBM MQ Windows*

Heslo pro účet lokálního uživatele 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 , proveďte následující kroky:

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 **Přihlásit** .
6. Potvrďte, že se uvedený název účtu shoduje s uživatelem, pro který bylo heslo změněno.
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 produktu Prepare IBM MQ Wizard k zadání podrobností o účtu uživatele domény můžete použít panel Správa počítačů ke změně podrobností **Přihlásit** pro specifickou službu IBM MQ pro instalaci.

Informace o této úloze

Je-li služba IBM MQ Windows pro instalaci spuštěna pod uživatelským účtem domény, můžete změnit heslo účtu takto:

Postup

1. Změňte heslo pro účet domény na řadiči domény. Možná budete muset požádat administrátora domény, aby to pro vás udělal.
2. Postupujte takto, chcete-li upravit stránku **Přihlášení** pro službu IBM MQ .
   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 **Přihlásit** .
   f) Potvrďte, že se uvedený název účtu shoduje s uživatelem, pro který bylo heslo změněno.
   g) Zadejte heslo do polí **Heslo** a **Potvrdit heslo** a klepněte na tlačítko **OK**.

   Uživatelský účet, který služba IBM MQ Windows spouští, provádí všechny příkazy MQSC, které jsou vydány aplikacemi uživatelského rozhraní, nebo jsou prováděny automaticky při spuštění systému, ukončení práce systému nebo zotavení služby. Tento uživatelský účet musí mít proto oprávnění k administraci produktu IBM MQ . Standardně je tento příkaz přidán do lokální skupiny mqm na serveru. Je-li toto členství odebráno, služba IBM MQ Windows nebude fungovat. Další informace o uživatelských právech najdete v tématu “Uživatelská práva vyžadovaná pro službu IBM MQ Windows Service” na stránce 145.

   Pokud se vyskytne problém zabezpečení s účtem uživatele, pod kterým je služba IBM MQ Windows spuštěna, objeví se chybové zprávy a popisy v protokolu systémových událostí.

Související úlohy

Konfigurace produktu IBM MQ s produktem Prepare IBM MQ Wizard

Windows *Aspekty podpory serverů Windows na řadiče domény*

Při povýšení serveru Windows na řadič domény byste měli zvážit, zda je vhodné nastavení zabezpečení týkající se oprávnění uživatele a skupiny. Při změně stavu počítače Windows mezi serverem a řadičem domény byste měli vzít v úvahu, že toto může ovlivnit provoz produktu IBM MQ , protože produkt IBM MQ používá lokálně definovanou skupinu mqm.

Nastavení zabezpečení týkající se oprávnění uživatelů domény a skupinových oprávnění

IBM MQ spoléhá na informace o členství ve skupinách k implementaci své zásady zabezpečení, což znamená, že je důležité, aby ID uživatele, které provádí operace IBM MQ , určilo členství ve skupině ostatních uživatelů.

Povýšíte-li server Windows na řadič domény, zobrazí se vám volba pro nastavení zabezpečení týkající se oprávnění uživatelů a skupin. Tato volba určuje, zda lze z aktivního adresáře načíst členství ve skupině (arbitrární). Pokud je řadič domény nastaven tak, aby lokální účty měly oprávnění k dotazování na členství ve skupinách uživatelských účtů domény, může výchozí ID uživatele vytvořené IBM MQ během instalačního procesu získat členství ve skupině pro ostatní uživatele, jak je požadováno. Je-li však řadič

domény nastaven tak, aby lokální účty neměly oprávnění k dotazování na členství ve skupinách pro uživatelské účty domény, zabrání to IBM MQ provedením kontrol, že uživatelé, kteří jsou definováni v doméně, jsou autorizováni pro přístup ke správcům front nebo frontám a přístup selže. Používáte-li Windows na řadiči domény, který byl nastaven tímto způsobem, musí se použít speciální doménový uživatelský účet s požadovanými oprávněními.

V tomto případě byste měli vědět:

- Jak se chovají oprávnění zabezpečení pro vaši verzi produktu Windows .
- Jak povolit členům skupiny mqm v doméně čtení členství ve skupině.
- Jak nakonfigurovat službu IBM MQ Windows ke 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 jsou z nich vyřazovány, produkt IBM MQ ztratí přístup k lokální skupině mqm.

Je-li server povýšen na řadič domény, změní se rozsah z lokální na lokální doménu. Když je počítač degradován na server, všechny lokální skupiny domény se odeberou. To znamená, že změna počítače ze serveru na řadič domény a zpět na server ztratí přístup k lokální skupině mqm. Příznakem je chyba označující nepřítomnost 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 správy produktu Windows . Protože jsou všechny informace o členství ve skupinách ztraceny, musíte obnovit privilegované uživatele IBM MQ v nově vytvořené lokální skupině mqm. Je-li počítač členem domény, musíte také přidat skupinu mqm domén do lokální skupiny mqm, aby bylo možné udělit ID uživatele privilegované domény IBM MQ požadovanou úroveň oprávnění.

Windows *Omezení ve vnořených skupinách v systému Windows*

Pro použití vnořených skupin existují omezení. Tyto výsledky částečně pocházejí z funkční úrovně domény a částečně z omezení IBM MQ .

Volba Active Directory může podporovat různé typy skupin v rámci kontextu domény v závislosti na funkční úrovni domény. Ve výchozím nastavení jsou domény Windows 2003 v " Windows 2000 smíšená " funkční úroveň. (Windows Server 2008 a Windows Server 2012 následujte model domény Windows 2003 .) Funkční úroveň domény určuje podporované typy skupin a úroveň vnoření povolených při konfiguraci ID uživatelů v prostředí domény. Podrobnosti o kritériích rozsahu skupiny a zařazení najdete v dokumentaci k produktu Active Directory .

Kromě požadavků Active Directory jsou uložena další omezení ID používaných produktem IBM MQ. Síťová rozhraní API používaná produktem IBM MQ nepodporují všechny konfigurace, které jsou podporovány funkční úrovní domény. V důsledku toho se produkt IBM MQ nemůže dotázat na členství ve skupině žádného ID domény přítomných v lokální skupině domény, která je poté vnořena v lokální skupině. Navíc vícenásobné vnoření globálních a univerzálních skupin není podporováno. Jsou však podporovány okamžitě vnořené globální nebo univerzální skupiny.

Windows *Autorizování uživatelů pro vzdálené použití produktu IBM MQ*

Potřebujete-li vytvořit a spustit správce front při vzdáleném připojení k produktu IBM MQ , musíte mít k dispozici uživatelský přístup `Vytvořit globální objekty` .

Informace o této úloze

Poznámka: Administrátoři mají při výchozím nastavení přístup uživatele `Vytvořit globální objekty` , takže pokud jste administrátorem, můžete vytvářet a spouštět správce front při vzdáleném připojení, aniž by došlo ke změně vašich uživatelských práv.

Pokud se připojujete k počítači s produktem Windows pomocí služeb Terminal Services nebo Remote Desktop Connection a máte problémy s vytvářením, spouštěním nebo odstraněním správce front, může to být způsobeno tím, že nemáte přístup uživatele `Vytvořit globální objekty`.

Uživatelský přístup `Vytvořit globální objekty` omezuje uživatele, kteří mají oprávnění k vytváření objektů v globálním oboru názvů. Má-li aplikace vytvořit globální objekt, musí být buď spuštěn v globálním oboru názvů, nebo uživatel, pod kterým je spuštěna aplikace, musí mít na něj použitý uživatelský přístup `Vytvořit globální objekty` .

Když se připojujete vzdáleně k počítači se systémem Windows pomocí služeb Terminal Services nebo Remote Desktop Connection, aplikace běží ve svém vlastním lokálním oboru názvů. If you attempt to create or delete a queue manager using IBM MQ Explorer or the **crtmqm** or **dltmqm** command, or to start a queue manager using the **strmqm** command, it results in an authorization failure. Tím se vytvoří FDC IBM MQ s ID sondy XY132002.

Spuštění správce front pomocí příkazu IBM MQ Explorernebo použití příkazu **amqmdain qmgr start** funguje správně, protože tyto příkazy přímo nespouští správce front. Místo toho příkazy odešlou požadavek na spuštění správce front do samostatného procesu spuštěného v globálním oboru názvů.

Pokud různé metody administrace IBM MQ nefungují při použití terminálových služeb, pokuste se nastavit uživatele `Vytvořit globální objekty` správně.

Postup

1. Otevřete panel Administrativní nástroje:

   Windows Server 2008 a Windows Server 2012
   Tento panel otevřete pomocí nabídky **Ovládací panely** > **Systém a údržba** > **Administrativní nástroje**.

   Windows 8.1
   Otevřete tento panel pomocí nabídky **Administrativní nástroje** > **Správa počítačů** .
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 *Ukončovací program kanálu SSPI v systému Windows*

Produkt IBM MQ for Windows poskytuje uživatelský program zabezpečení, který lze použít pro kanály zpráv i pro kanály MQI. Ukončení je dodáno jako zdrojový a objektový kód a poskytuje jednosměrně a dvoucestné ověření.

Uživatelská procedura zabezpečení používá rozhraní SSPI (Security Support Provider Interface), které poskytuje integrované bezpečnostní mechanizmy platforem Windows .

Uživatelská procedura zabezpečení poskytuje následující služby identifikace a ověření:

jednosměrné ověření
To používá podporu ověření produktu Windows NT LAN Manager (NTLM). NTLM umožňuje serverům autentizovat své klienty. Neumožňuje klientovi ověřit identitu serveru nebo jeden server pro ověření jiného serveru. NTLM byl navržen pro síťové prostředí, ve kterém se předpokládá, že servery jsou pravé. NTLM je podporováno na všech platformách Windows , které jsou podporovány produktem IBM WebSphere MQ 7.0.

Tato služba se zpravidla používá na kanálu MQI k povolení správce front serveru pro ověření aplikace IBM MQ MQI client . Klientská aplikace je identifikována pomocí ID uživatele přidruženého k procesu, který je spuštěn.

Chcete-li provést ověření, uživatelská procedura zabezpečení na straně klienta kanálu získá token ověření z NTLM a odešle token ve zprávě zabezpečení svému partnerovi na druhém konci kanálu. Uživatelská procedura zabezpečení partnera předá token do NTLM, který kontroluje, zda je token

autentický. Pokud uživatelská procedura pro zabezpečení partnera není s autenticitou tokenu spokojena, dává pokyn programu MCA k uzavření kanálu.

Dva způsoby, nebo vzájemné, ověření
To 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 pro kanály MQI. Na kanálu zpráv poskytuje vzájemné ověření těchto dvou správců front. Na kanálu MQI je možné, aby se správce front serveru a aplikace IBM MQ MQI client vzájemně ověřovali. Správce front je identifikován svým názvem s předponou řetězcem `ibmMQSeries/`. Klientská aplikace je identifikována pomocí ID uživatele přidruženého k procesu, který je spuštěn.

Chcete-li provést vzájemné ověření, iniciující uživatelská procedura zabezpečení získá ověřovací token ze serveru zabezpečení Kerberos a odešle token ve zprávě zabezpečení svému partnerovi. Uživatelská procedura zabezpečení ochrany dat předá token serveru Kerberos , který zkontroluje, že je autentický. Server zabezpečení Kerberos generuje druhý token, který partner odešle ve zprávě o zabezpečení do inicializační uživatelské procedury zabezpečení. Zahajující uživatelská procedura zabezpečení poté požádá server Kerberos o kontrolu autentických znaků druhého tokenu. Pokud během této výměny není ukončena žádná uživatelská procedura zabezpečení s autenticitou tokenu odeslaného druhým z nich, dává programu MCA pokyn k uzavření kanálu.

Uživatelská procedura zabezpečení je dodávána ve formátu zdroje i objektu. Zdrojový kód můžete použít jako výchozí bod pro zápis vašich vlastních ukončovacích programů kanálu nebo můžete použít objektový modul jako dodaný. Modul objektu má dva vstupní body, jeden pro jednosměrné ověření pomocí podpory ověření NTLM a druhý pro dvousměrné ověření pomocí ověřovacích služeb Kerberos .

Další informace o tom, jak pracuje program výstupního bodu kanálu SSPI a instrukce, jak jej implementovat, najdete v tématu Použití uživatelské procedury zabezpečení SSPI v systémech Windows.

Windows *Použití souborů šablon zabezpečení v systému Windows*

Použití šablony může ovlivnit nastavení zabezpečení použité pro soubory a adresáře produktu IBM MQ . Používáte-li vysoce zabezpečenou šablonu, použijte ji před instalací produktu IBM MQ.

Produkt Windows podporuje soubory šablon zabezpečení založených na textu, které můžete použít k použití uniformních nastavení zabezpečení pro jeden nebo více počítačů s modulem snap-in Konfigurace zabezpečení a analýzy MMC. Produkt Windows poskytuje zejména několik šablon, které obsahují celou řadu nastavení zabezpečení s cílem poskytovat specifické úrovně zabezpečení. Tyto šablony zahrnují Kompatibilní, Zabezpečené a Vysoce zabezpečené.

Použití jedné z těchto šablon může mít vliv na nastavení zabezpečení aplikovaná na soubory a adresáře produktu IBM MQ . Chcete-li použít šablonu Vysoce Secure, nakonfigurujte počítač před instalací produktu IBM MQ.

Pokud použijete vysoce zabezpečenou šablonu na počítač, na kterém je již produkt IBM MQ nainstalován, budou odebrána všechna oprávnění, která jste nastavili u souborů a adresářů produktu IBM MQ . Protože tato oprávnění jsou odebrána, ztratíte uživatele *Administrator*, *mqm*a v případě potřeby přístup skupiny *Everyone* z chybových adresářů.

Windows *Konfigurace dodatečného oprávnění pro aplikace produktu Windows připojující se k produktu IBM MQ*

Účet, pod kterým mohou být spuštěny procesy produktu IBM MQ , může vyžadovat dodatečné oprávnění dříve, než může být udělen přístup k procesům aplikace SYNCHRONIZE k procesům aplikace.

Informace o této úloze

Mohou se vyskytnout problémy, pokud máte aplikace Windows , například stránky ASP, připojení k serveru IBM MQ , které jsou konfigurovány pro spuštění na úrovni zabezpečení vyšší, než je obvyklé.

IBM MQ vyžaduje přístup SYNCHROIZE k procesům aplikace za účelem koordinace určitých akcí. Když se serverová aplikace nejprve pokusí připojit ke správci front IBM MQ , upraví proces tak, aby udělil oprávnění SYNCHRONIZE pro administrátory produktu IBM MQ . Avšak účet, pod kterým jsou spuštěny procesy produktu IBM MQ , může vyžadovat další oprávnění, dříve než může být udělen požadovaný přístup.

Chcete-li konfigurovat další oprávnění k ID uživatele, pod kterým jsou procesy produktu IBM MQ spuštěny, postupujte takto:

Postup

1. Spusťte nástroj Lokální zásady zabezpečení, klepněte na **Nastavení zabezpečení**->**Lokální zásady**->**Přiřazení uživatele**, klepněte na **Ladit programy**.
2. Poklepejte na položku **Ladit programy**a poté do seznamu přidejte ID uživatele produktu IBM MQ .

   Pokud se systém nachází v doméně Windows a nastavení efektivní zásady stále není nastaveno, i když je nastaveno lokální nastavení zásad, musí být ID uživatele autorizováno stejným způsobem na úrovni domény, pomocí nástroje zásad zabezpečení domény.

IBM i Nastavení zabezpečení v systému IBM i

Zabezpečení v produktu IBM i je implementováno pomocí zabezpečení na úrovni objektů IBM MQ Object Authority Manager (OAM) a IBM i (Object Authority Manager).

Aspekty zabezpečení, které musí být provedeny při určování přístupových oprávnění k objektům produktu IBM MQ .

Při nastavování oprávnění pro uživatele ve vašem podniku je třeba zvážit následující skutečnosti:

1. Udělte a zrušte oprávnění k příkazům IBM MQ for IBM i pomocí příkazů IBM i GRTOBJAUT a RVKOBJAUT .

   V knihovně produktu QMQM jsou určité objekty noncommand (* cmd) nastaveny tak, aby měly oprávnění ***PUBLIC** k ***USE**. Neměňte oprávnění těchto objektů, nebo pro poskytnutí oprávnění použijte seznam oprávnění. Jakékoli nesprávné oprávnění může ohrozit funkčnost produktu IBM MQ .
2. Během instalace produktu IBM MQ for IBM ijsou vytvořeny následující speciální profily uživatelů:

   QMQM
   Používá se primárně pro interní funkce produktu. Lze ji však použít ke spuštění důvěryhodných aplikací pomocí funkce MQCNO_FASTPATH_BINDINGS. Viz Připojení ke správci front pomocí volání MQCONNX.

   QMQMADM
   Je použit jako skupinový profil pro administrátory produktu IBM MQ. Profil skupiny poskytuje přístup k CL příkazům a prostředkům IBM MQ .

   Když používáte SBMJOB k odeslání programů, které volají příkazy IBM MQ , USER nesmí být výslovně nastaveno na QMQMADM. Místo toho nastavte USER na QMQM nebo jiný uživatelský profil, který má uvedeno QMQMADM jako skupinu.
3. Pokud odesíláte příkazy kanálu ke vzdáleným správcům front, ujistěte se, že váš profil uživatele je členem skupiny QMQMADM na cílovém systému. Seznam příkazů kanálů PCF a MQSC naleznete v příručce IBM MQ for IBM i CL commands.
4. Sada skupin přidružená k uživateli je uložena do mezipaměti, když jsou autorizace skupiny vypočítány pomocí OAM.

   Všechny změny provedené v členství uživatele ve skupinách po nastavení skupiny do mezipaměti nebudou rozpoznány, dokud správce front nerestartujete nebo nespustíte příkaz RFRMQMAUT k obnovení zabezpečení.
5. Omezte počet uživatelů, kteří mají oprávnění pracovat s příkazy, které jsou zvláště citlivé. Tyto příkazy zahrnují:

   - Vytvoření správce front zpráv (CRTMQM)

- Výmaz správce front zpráv (DLTMQM)
- Spuštění správce front zpráv (STRMQM)
- Ukončení správce front zpráv (ENDMQM)
- STRMQMCSVR (Spuštění příkazového serveru)
- Ukončení příkazového serveru (ENDMQMCSVR)

6. Definice kanálů obsahují specifikaci ukončovacího programu zabezpečení. Vytvoření a úprava kanálu vyžaduje speciální ohledy. Podrobnosti o uživatelských procedurách zabezpečení jsou uvedeny v “Přehled uživatelské procedury zabezpečení” na stránce 104.
7. Je možné nahradit programy pro ukončení kanálu a spouštěcí programy spouštěčů. Za bezpečnost těchto výměn je odpovědný programátor.

IBM i Správce oprávnění objektu v systému IBM i

Správce oprávnění objektu (OAM) spravuje autorizace uživatelů pro manipulaci s objekty produktu IBM MQ , včetně front a definic procesů. Poskytuje také rozhraní příkazového řádku, jehož prostřednictvím můžete udělovat nebo odvolávat přístupová oprávnění k objektu pro určitou skupinu uživatelů. Rozhodnutí o povolení přístupu k prostředku je provedeno pomocí OAM a správce front toto rozhodnutí dodržuje. Pokud OAM nemůže učinit rozhodnutí, zabrání správci front přístup k tomuto prostředku.

Prostřednictvím OAM můžete řídit:

- Přístup k objektům produktu IBM MQ prostřednictvím rozhraní MQI. Když se aplikační program pokusí o přístup k objektu, OAM zkontroluje, zda má profil uživatele, zda má požadavek, oprávnění pro požadovanou operaci.

  To znamená, že to 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 různé přístupové oprávnění ke stejnému objektu. Například u určité fronty může jedna skupina provádět operace put i get; jiná skupina může být povolena pouze pro procházení fronty (MQGET s volbou procházení). Podobně, některé skupiny mohou mít oprávnění k získání a vložení do fronty, ale nejsou povoleny změny nebo odstranění fronty.

Příkazy IBM MQ for IBM i a provádění operací na objektech IBM MQ for IBM i

IBM i Oprávnění IBM MQ v systému IBM i

Chcete-li přistupovat k objektům produktu IBM MQ , potřebujete oprávnění k vydání příkazu a k přístupu k odkazovanému objektu. Administrátoři mají přístup ke všem prostředkům produktu IBM MQ .

Přístup k objektům produktu IBM MQ je řízen oprávněními pro:

1. Zadejte příkaz IBM MQ .
2. Přístup k objektům produktu IBM MQ , na které příkaz odkazuje.

Všechny CL příkazy IBM MQ for IBM i se dodávají s vlastníkem QMQM a administrativní profil (QMQMADM) má oprávnění *USE k přístupu *PUBLIC nastaveným na *EXCLUDE.

Poznámka: Program QSRDUPER je používán instalačním programem IBM MQ pro licencovaný program IBM i k duplikaci objektů Command (*CMD) v QSYS. Ve verzi IBM i V5R4 a později byl program QSRDUPER změněn tak, aby předvolené chování bylo vytvořit příkaz proxy místo duplikátu původního příkazu. Příkaz proxy přesměruje provedení příkazu na jiný příkaz a má atribut PRX. Pokud příkaz proxy stejného názvu jako kopírovaný příkaz existuje v knihovně QSYS, soukromé oprávnění k příkazu proxy se neudělí příkazu v knihovně produktu. Pokusy o výzvu nebo spuštění příkazu proxy v QSYS kontrolují oprávnění cílového příkazu v knihovně produktu. Jakékoli změny v oprávnění k objektům *CMD proto musí být provedeny v knihovně produktu (QMQM) a ty v QSYS není třeba upravovat. Příklad:

```
GRTOBJAUT OBJ(QMQM/DSPMQMQ) OBJTYPE(*CMD) USER(MQUSER) AUT(*USE)
```

Změny struktury oprávnění u některých CL příkazů produktu umožňují veřejné použití těchto příkazů, pokud máte požadované oprávnění OAM k objektům IBM MQ , aby tyto změny byly provedeny.

Chcete-li být administrátorem produktu IBM MQ na systému IBM i, musíte být členem skupiny *QMQMADM*. Tato skupina má vlastnosti, jako jsou vlastnosti skupiny mqm na systémech AIX, Linux, and Windows . Konkrétně, skupina QMQMADM se vytvoří, když instalujete produkt IBM MQ for IBM i, a členové skupiny QMQMADM mají přístup ke všem prostředkům IBM MQ v systému. Máte-li oprávnění *ALLOBJ, máte také přístup ke všem prostředkům produktu IBM MQ .

Administrátoři mohou použít CL příkazy ke správě IBM MQ. Jedním z těchto příkazů je GRTMQMAUT, který se používá k udělování oprávnění jiným uživatelům. Jiný příkaz STRMQMMQSC umožňuje administrátorovi zadávat příkazy MQSC lokálnímu správci front.

Související pojmy

"Oprávnění ke správě produktu IBM MQ v systému IBM i" na stránce 84

IBM i *Přístupová oprávnění pro objekty IBM MQ v systému IBM i*

Přístupové oprávnění požadované pro spuštění CL příkazů IBM MQ .

IBM MQ for IBM i kategorizuje CL příkazy produktu do dvou skupin:

Skupina 1

Uživatelé musí být ve skupině uživatelů QMQMADM, nebo mít oprávnění *ALLOBJ ke zpracování těchto příkazů. Uživatelé, kteří mají některou z těchto oprávnění, mohou zpracovat všechny příkazy ve všech kategoriích, aniž by museli vyžadovat další oprávnění.

Poznámka: Tyto orgány přepisují jakékoli oprávnění OAM.

Tyto příkazy lze seskupit podle následujících pokynů:

- Příkazy příkazového serveru
  - ENDMQMCSVR, Ukončení příkazového serveru IBM MQ
  - STRMQMCSVR, Spuštění příkazového serveru IBM MQ
- Příkaz obslužné rutiny fronty nedoručených zpráv
  - STRMQMDLQ, Spuštění popisovače fronty IBM MQ nedoručitelných zpráv
- Příkaz modulu listener
  - ENDMQMLSR, Ukončení modulu listener produktu IBM MQ
  - STRMQMLSR, Spuštění neobjektového modulu listener
- Příkazy obnovy médií
  - RCDMQMIMG, Záznam obrazu objektu IBM MQ
  - RCRMQMOBJ, Re-create IBM MQ Objekt
  - WRKMQMTRN, práce s IBM MQ Q transakcemi
- Příkazy správce front
  - CRTMQM, Vytvoření správce front zpráv
  - DLTMQM, Výmaz 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, Trasování úlohy IBM MQ
- Příkazy pro transakce

  - RSVMQMTRN, Vyřešit transakci IBM MQ
- Příkazy monitoru spouštěčů
  - STRMQMTRM, Spuštění monitoru spouštěčů
- Příkazy SC produktu IBM MQ
  - RUNMQSC, spusťte příkazy produktu IBM MQSC
  - STRMQMMů, Spuštění příkazů produktu IBM MQSC

Skupina 2

Zbývající příkazy, pro které jsou požadovány dvě úrovně oprávnění:

1. Oprávnění IBM i ke spuštění příkazu. Administrátor serveru IBM MQ jej nastavuje pomocí příkazu **GRTOBJAUT** , aby přepsal omezení *PUBLIC 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, s ohledem na správné oprávnění IBM i v kroku 1.

   Toto oprávnění je řízeno uživatelem s příslušným oprávněním OAM pro požadovanou akci, kterou nastavil administrátor produktu IBM MQ pomocí příkazu **GRTMQMAUT** .

   Příklad:

   ```
   GRTMQMAUT *connect authority to the queue manager + *admchg authority to
           the queue
   ```

Příkazy lze seskupit podle následujících pokynů:

- Příkazy kanálu
  - CHGMQMCHL, změna kanálu IBM MQ

    To vyžaduje * oprávnění k připojení ke správci front a * admchg oprávnění ke kanálu.
  - CPYMQMCHL, kopírovat kanál IBM MQ

    To vyžaduje * connect and * admcrt authority to the queue manager, * admdsp authority to the default channel type to be copied, and * admccrt authority to the channel object class.

    Například kopírování odesílacího kanálu vyžaduje oprávnění * admdsp na SYSTEM.DEF.SENDER
  - CRTMQMCHL, Vytvořit kanál IBM MQ

    To vyžaduje * connect and * admcrt authority to the queue manager, * admdsp authority to the default channel type to be created and * admccrt authority to the channel object class.

    Například vytvoření kanálu odesílatele vyžaduje oprávnění * admdsp pro SYSTEM.DEF.SENDER
  - DLTMQMCHL, Výmaz kanálu IBM MQ

    To vyžaduje * oprávnění k připojení ke správci front a * admdlt oprávnění ke kanálu.
  - RSVMSQMCHL, Vyřešit kanál IBM MQ

    To vyžaduje * oprávnění k připojení ke správci front a * ctrlx oprávnění ke kanálu.
- Zobrazit příkazy

  Chcete-li zpracovat příkazy DSP, musíte udělit uživateli oprávnění `*connect` a `*admdsp` správci front společně s libovolnou specifickou uvedenou volbou:
  - DSPMQM, Zobrazení správce front zpráv
  - DSPMQMAUT, Zobrazení oprávnění k objektu IBM MQ

  - DSPMQMAUTI, Zobrazení ověřovacích informací IBM MQ - *admdsp na objekt ověřovacích informací
  - DSPMQMCHL, Zobrazení kanálu IBM MQ - *admdsp na kanál
  - DSPMQMCSVR, Zobrazení příkazového serveru IBM MQ
  - DSPMQMNL, Zobrazení seznamu názvů IBM MQ - *admdsp na seznam názvů
  - DSPMQMOVBN, Zobrazení názvů objektů IBM MQ
  - DSPMQMPRC, Zobrazení IBM MQ procesu- *admdsp na proces
  - DSPMQMQ, Zobrazení fronty IBM MQ - *admdsp do fronty
  - DSPMQMTOP, Zobrazit téma IBM MQ - *admdsp na téma
- Práce s příkazy

  Chcete-li zpracovat příkazy WRK a zobrazit panel s volbami, musíte udělit uživateli oprávnění *connect a *admdsp správci front společně s libovolnou specifickou uvedenou volbou:

  - 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 objekt ověřovacích informací IBM MQ .
    - *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 Clear IBM MQ Channel.
    - *admcrt pro příkaz Vytvořit a kopírovat kanál IBM MQ .
    - *admdlt pro příkaz Delete IBM MQ Channel.
    - *admdsp pro příkaz Display IBM MQ Channel.
    - *ctrl pro příkaz Start IBM MQ Channel.
    - *ctrl pro příkaz End IBM MQ Channel.
    - *ctrl pro příkaz Ping IBM MQ Channel.
    - *ctrlx pro příkaz Reset kanálu IBM MQ .
    - *ctrlx pro příkaz Vyřešit kanál IBM MQ .
  - WRKMQMCHST, Práce se stavem kanálu IBM MQ

    To vyžaduje oprávnění *admdsp ke kanálu.
  - WRKMQMCL, práce s klastry IBM MQ
  - WRKMQMCLQ, Práce s frontami klastru IBM MQ
  - 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 ke frontě
  - WRKMQMNL, Práce s IBM MQ seznamy názvů

    To vyžaduje následující oprávnění:

    - *admchg pro příkaz Změna seznamu názvů IBM MQ .

- *admcrt pro příkaz Vytvořit a kopírovat seznam názvů IBM MQ .
- *admdlt pro příkaz Odstranit seznam názvů IBM MQ .
- *admdsp pro příkaz Zobrazení seznamu názvů IBM MQ .

– WRKMQMPRC, práce s procesy IBM MQ

To vyžaduje následující oprávnění:

- *admchg pro příkaz Změnit proces IBM MQ .
- *admcrt pro příkaz Vytvořit a kopírovat proces IBM MQ .
- *admdlt pro příkaz Odstranit proces IBM MQ .
- *admdsp pro příkaz Display IBM MQ Process.

– WRKMQMQ, práce s frontami IBM MQ

To vyžaduje následující oprávnění:

- *admchg pro příkaz Změnit frontu IBM MQ .
- *admclr pro příkaz Vymazat frontu IBM MQ .
- *admcrt pro příkaz Vytvořit a kopírovat frontu IBM MQ .
- *admdlt pro příkaz Odstranit frontu IBM MQ .
- *admdsp pro příkaz Zobrazení fronty IBM MQ .

– WRKMQMQSTS, Práce se stavem fronty IBM MQ

– WRKMQMTOP, Práce s tématy IBM MQ

To vyžaduje následující oprávnění

- *admchg pro příkaz Změnit téma IBM MQ .
- *admcrt pro příkaz Vytvořit a kopírovat téma IBM MQ .
- *admdlt pro příkaz Odstranit téma IBM MQ .
- *admdsp pro příkaz Display IBM MQ Topic.

– WRKMQMSUB, práce s odběry IBM MQ

• Další příkazy kanálu

Chcete-li zpracovat příkazy kanálu, musíte udělit uživateli uvedené specifické oprávnění:

– ENDMQMCHL, Ukončit IBM MQ kanál

To vyžaduje oprávnění *connect ke správci front a oprávnění *allmqi k přenosové frontě přidružené k kanálu.

– ENDMQMLSR, Ukončení listeneru IBM MQ

To vyžaduje oprávnění *connect ke správci front a oprávnění správce *ctrl k uvedenému objektu modulu listener.

– PNGMQMCHL, Ping IBM MQ kanál

To vyžaduje oprávnění *connect a *inq ke správci front a oprávnění správce *ctrl k objektu kanálu.

– RSTMQMCHL, Resetovat kanál IBM MQ

To vyžaduje oprávnění *connect ke správci front.

– STRMQMCHL, spuštění kanálu IBM MQ

To vyžaduje oprávnění *connect ke správci front a oprávnění správce *ctrl k objektu kanálu.

– STRMQMCHLI, Spuštění iniciátoru kanálu IBM MQ

To vyžaduje oprávnění *connect a *inq pro správce front a oprávnění správce *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 uvedenému objektu listeneru.

- Další příkazy:

  Chcete-li zpracovat následující příkazy, musíte udělit uživateli uvedené specifické oprávnění:

  – CCTMQM, připojte se 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, Změna seznamu názvů IBM MQ

    To vyžaduje oprávnění `*connect` ke správci front a oprávnění `*admchg` k seznamu názvů.

  – CHGMQMPRC, Změna IBM MQ procesu

    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` k frontě.

  – CLRMQMQ, Vymazat frontu IBM MQ

    To vyžaduje oprávnění `*connect` ke správci front a oprávnění `*admclr` k frontě.

  – CPYMQMAUTI, kopírování ověřovacích informací IBM MQ

    To vyžaduje oprávnění `*connect` ke správci front a oprávnění `*admdsp` k objektu ověřovacích informací a oprávnění `*admcrt` k třídě objektů ověřovacích informací.

  – CPYMQMNL, Kopírovat seznam názvů IBM MQ

    To vyžaduje oprávnění `*connect` a `*admcrt` ke správci front.

  – CPYMQMPRC, kopírovat proces 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, vytvoření ověřovacích informací IBM MQ

    To vyžaduje oprávnění `*connect` ke správci front a oprávnění `*admdsp` k objektu ověřovacích informací a oprávnění `*admcrt` k třídě objektů ověřovacích informací.

  – CRTMQMNL, Vytvoření seznamu názvů IBM MQ

    To vyžaduje oprávnění `*connect` a `*admcrt` pro správce front a oprávnění správce `*admdsp` k výchozímu seznamu názvů.

  – CRTMQMPRC, Vytvoření procesu IBM MQ

    To vyžaduje oprávnění `*connect` a `*admcrt` ke správci front a oprávnění `*admdsp` k výchozímu procesu.

  – CRTMQMQ, Vytvoření fronty IBM MQ

    To vyžaduje oprávnění `*connect` a `*admcrt` pro správce front a oprávnění správce `*admdsp` k výchozí frontě.

  – CVTMQMDTA, Převést příkaz datového typu IBM MQ

    To nevyžaduje žádné oprávnění k objektu IBM MQ .

  – DLTMQMAUTI, Výmaz ověřovacích informací IBM MQ

To vyžaduje oprávnění *connect ke správci front a oprávnění *ctrlx k objektu ověřovacích informací.

– DLTMQMNL, Výmaz seznamu názvů IBM MQ

  To vyžaduje oprávnění *connect ke správci front a oprávnění *admdlt k seznamu názvů.

– DLTMQMPRC, odstranit proces IBM MQ

  To vyžaduje oprávnění *connect ke správci front a oprávnění *admdlt k procesu.

– DLTMQMQ, Výmaz fronty IBM MQ

  To vyžaduje oprávnění *connect ke správci front a oprávnění *admdlt k frontě.

– DSCMQM, odpojení od správce front zpráv

  To nevyžaduje žádné oprávnění k objektu IBM MQ .

– RFRMQMAUT, Aktualizovat zabezpečení

  To vyžaduje oprávnění *connect ke správci front.

– RFRMQMCL, Aktualizovat klastr

  To vyžaduje oprávnění *connect ke správci front.

– RSMMQMCLQM, Obnovit správce front klastru

  To vyžaduje oprávnění *connect ke správci front.

– RSTMQMCL, Resetovat klastr

  To vyžaduje oprávnění *connect ke správci front.

– SPDMQMCLQM, pozastavení správce front klastru

  To vyžaduje oprávnění *connect ke správci front.

IBM i *Oprávnění pro přístup k produktu IBM i*

Tyto informace vám pomohou porozumět příkazům autorizace přístupu.

Oprávnění definované klíčovým slovem AUT na příkazech GRTMQMAUT a RVKMQMAUT lze kategorizovat takto:

- Oprávnění související s voláními MQI
- Příkazy administrace související s autorizací
- Kontextové autorizace
- Obecné autorizace, tj. volání MQI, příkazů nebo obojího.

V následujících tabulkách jsou uvedeny různé oprávnění použitím parametru AUT pro volání MQI, volání kontextu, příkazy MQSC a PCF a generické operace.

Tabulka 15. Oprávnění pro volání MQI

AUT.	**Popis**
*ALTUSR	Povolit použití oprávnění jiného uživatele pro volání MQOPEN a MQPUT1 .
*BROWSE	Načtěte zprávu z fronty zadáním volání MQGET s volbou BROWSE.
*CONNECT	Připojení aplikace k zadanému správci front zadáním volání MQCONN.
*GET	Načtení zprávy z fronty zadáním volání MQGET.
*INQ	Vytvoření dotazu pro konkrétní frontu zadáním volání MQINQ.
*PUB	Chcete-li publikovat zprávu pomocí volání MQPUT, otevřete téma.
*PUT	Vložit zprávu do určité fronty zadáním volání MQPUT.
*RESUME	Obnovte odběr pomocí volání MQSUB.

Tabulka 15. Oprávnění pro volání MQI (pokračování)	
AUT.	**Popis**
*SET	Nastavte atributy ve frontě z rozhraní MQI zadáním volání MQSET. Pokud otevřete frontu pro více voleb, musíte být autorizováni pro každý z nich.
*SUB	Vytvořit, změnit nebo obnovit odběr u tématu pomocí volání MQSUB.

Tabulka 16. Autorizace pro volání kontextu	
AUT.	**Popis**
*PASSALL	Propustit celý kontext na uvedené frontě. Všechna pole kontextu se zkopírují z původního požadavku.
*PASSID	Předat kontext identity na zadané frontě. Kontext identity je stejný jako kontext požadavku.
*SETALL	Nastavit celý kontext na zadané frontě. Toto je používáno speciálními systémovými obslužnými programy.
*SETID	Nastavit kontext identity na zadané frontě. Toto je používáno speciálními systémovými obslužnými programy.

Tabulka 17. Oprávnění pro volání MQSC a PCF	
AUT.	**Popis**
*ADMCHG	Změnit atributy uvedeného objektu.
*ADMCLR	Vymažte uvedený objekt (pouze příkaz objektu PCF Clear).
*ADMCRT	Vytvořte objekty uvedeného typu.
*ADMDLT	Vymažte uvedený objekt.
*ADMDSP	Zobrazí atributy uvedeného objektu.

Tabulka 18. Oprávnění pro generické operace	
AUT.	**Popis**
*ALL	Použít všechny operace použitelné pro objekt. Oprávnění `all` se rovná sjednocení oprávnění `alladm`, `allmqia` `system` odpovídající danému typu objektu.
*ALLADM	Provádět všechny administrační operace vztahující se na objekt.
*ALLMQI	Použít všechna volání MQI použitelná pro objekt.
*CTRL	Řídit spuštění a ukončení kanálů, listenerů a služeb.
*CTRLX	Obnovte pořadové číslo a vyřešte nejisté kanály.

IBM i *Použití příkazů autorizace přístupu v systému IBM i*

Tyto informace použijte k získání informací o příkazech pro autorizaci přístupu a k použití příkladů příkazů.

Použití příkazu GRTMQMAUT

Máte-li požadovanou autorizaci, můžete pomocí příkazu GRTMQMAUT udělit autorizaci profilu uživatele nebo skupiny uživatelů pro přístup k určitému objektu. Následující příklady ilustrují způsob 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 jméno uživatelského profilu na systému, pro který se autorizace mění. Tento profil může být použit jako skupinový profil pro ostatní uživatele.
   - *BROWSE a *PUT jsou autorizace, která jsou udělena pro uvedenou frontu.

     Produkt *BROWSE přidá autorizaci k procházení zpráv ve frontě (aby bylo možné zadat příkaz MQGET s volbou procházení).

     Příkaz *PUT přidá do fronty oprávnění pro vkládání zpráv (MQPUT).
   - saturn.queue.manager je název správce front.
2. Následující příkaz uděluje uživatelům JACK a JACK všechny příslušné autorizace pro všechny definice procesů, pro výchozího správce front.

```
GRTMQMAUT OBJ(*ALL) OBJTYPE(*PRC) USER(JACK JILL) AUT(*ALL)
```

3. Následující příkaz udělí uživateli GEORGE oprávnění k vložení zprávy 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 požadované oprávnění, můžete pomocí příkazu RVKMQMAUT odebrat dříve udělené oprávnění profilu uživatele nebo skupiny uživatelů pro přístup k určitému objektu. Následující příklady ilustrují způsob použití příkazu RVKMQMAUT :

1.
```
RVKMQMAUT OBJ(RED.LOCAL.QUEUE) OBJTYPE(*LCLQ) USER(GROUPA) +
AUT(*PUT) MQMNAME('saturn.queue.manager')
```

   Oprávnění k vložení zpráv do zadané 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 získání zpráv z libovolné fronty s názvem začínajícím znaky PAYvlastněnými správcem front PAYROLLQMje odebráno ze všech uživatelů systému, pokud tyto osoby nebo skupina, do které patří, nebyly samostatně autorizovány.

Použití příkazu DSPMQMAUT

Zobrazení oprávnění MQM (DSPMQMAUT) uvádí, pro uvedený objekt a uživatele, seznam oprávnění, která má uživatel pro daný 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) příkaz umožňuje okamžitou aktualizaci informací o skupině autorizace produktu OAM, což odráží změny provedené na úrovni operačního systému, aniž by bylo nutné zastavit a znovu spustit správce front. Následující příklad ukazuje, jak se příkaz používá:

```
RFRMQMAUT MQMNAME(ADMINQM)
```

IBM i Tabulky specifikací autorizace v systému IBM i

Pomocí těchto informací můžete určit, která autorizace je nezbytná pro použití konkrétních volání rozhraní API, a konkrétní volby těchto volání, objektů fronty, objektů procesu a objektů správce front.

Tabulky specifikace autorizace začínající v produktu Tabulka 19 na stránce 162 definují přesně, jak fungují autorizace, a omezení, která platí. Tabulky se vztahují na tyto situace:

- Aplikace, které vydávají volání MQI
- Administrační programy, které vydávají příkazy MQSC jako escape PCF
- Administrační programy, které vydávají příkazy PCF

V tomto oddílu jsou informace prezentovány jako sada tabulek, které určují následující údaje:

Akce, která se má provést
Volba MQI, příkaz MQSC nebo příkaz PCF.

Objekt řízení přístupu
Queue, process definition, queue manager, namelist, channel, client connection channel, listener, service, or authentication information object.

Je vyžadována autorizace
Vyjádřeno jako konstanta MQZAO_.

V tabulkách odpovídají předponě předponou MQZAA_ klíčová slova v seznamu oprávnění pro příkazy **GRTMQMAUT** a **RVKMQMAUT** pro konkrétní entitu. Například MQZA_BROWSE odpovídá klíčovému slovu *BROWSE ; Podobně klíčové slovo MQZAO_SET_ALL_CONTEXT odpovídá klíčovému slovu *SETALLa tak dále. Tyto konstanty jsou definovány v souboru záhlaví cmqzc.h, který se dodává spolu s produktem.

Autorizace MQI

Aplikace může vydat specifická volání a volby MQI pouze v případě, že je daný identifikátor uživatele, pod kterým je spuštěn (nebo jehož autorizace lze předpokládat), udělena příslušná autorizace.

Čtyři volání MQI vyžadují kontroly autorizace: MQCONN, MQOPEN, MQPUT1a MQCLOSE.

Pro MQOPEN a MQPUT1je kontrola oprávnění provedena na názvu objektu, který je otevíraný, a nikoli na názvu, nebo názvech, které jsou výsledkem názvu, který byl vyřešen. Například aplikaci může být uděleno oprávnění k otevření fronty alias bez oprávnění k otevření základní fronty, na kterou je alias interpretováno. Pravidlem je, že kontrola se provádí na první definici zjištěné během procesu rozpoznání názvu, který není alias správce front, pokud definice alias správce front není otevřena přímo; to znamená, že jeho název je zobrazen v poli *ObjectName* deskriptoru objektu. Oprávnění je vždy potřebné pro otevřený objekt. V některých případech je vyžadováno další oprávnění nezávislé na frontě, získané prostřednictvím autorizace pro objekt správce front.

Tabulka 19 na stránce 162, Tabulka 20 na stránce 162, Tabulka 21 na stránce 163a Tabulka 22 na stránce 163 sumarizují oprávnění potřebná pro každé volání.

Poznámka: Tyto tabulky neuvádějí názvy seznamů názvů, kanálů, kanálů připojení klienta, modulů listener, služeb nebo objektů ověřovacích informací. Důvodem je to, že se na tyto objekty nevztahují žádná oprávnění, s výjimkou MQOO_INQUIRE, pro které platí stejná oprávnění jako pro ostatní objekty.

Tabulka 19. Autorizace zabezpečení potřebná pro volání MQCONN			
Je vyžadována autorizace pro:	**Objekt fronty (“1” na stránce 163)**	**Objekt procesu**	**Objekt správce front**
Volba MQCONN	Nelze použít	Nelze použít	MQZAO_PŘIPOJENÍ

Tabulka 20. Autorizace zabezpečení potřebná pro volání MQOPEN			
Je vyžadována autorizace pro:	**Objekt fronty (“1” na stránce 163)**	**Objekt procesu**	**Objekt správce front**
MQO_ DOTÁZAT SE	MQZAO_INQUIRE **(“2” na stránce 163)**	MQZAO_INQUIRE **(“2” na stránce 163)**	MQZAO_INQUIRE **(“2” na stránce 163)**
MQOOK_BROWSE	MQZAO_BROWSE	Nelze použít	Žádná kontrola
MQO_INPUT_*	MQZAO_VSTUP	Nelze použít	Žádná kontrola
MQOO_SAVE_ ALL_CONTEXT **(“3” na stránce 163)**	MQZAO_VSTUP	Nelze použít	Nelze použít
MQOO_OUTPUT (normální fronta) **(“4” na stránce 163)**	MQZAO_VÝSTUP	Nelze použít	Nelze použít
MQOO_PASS_ IDENTITY_CONTEXT **(“5” na stránce 163)**	MQZAO_PASS_ IDENTITY_CONTEXT	Nelze použít	Žádná kontrola
MQOO_PASS_ALL_ CONTEXT **(“5” na stránce 163, “6” na stránce 163)**	MQZAO_PASS _ALL_CONTEXT	Nelze použít	Žádná kontrola
MQOO_SET_ IDENTITY_CONTEXT **(“5” na stránce 163, “6” na stránce 163)**	MQZAO_SET_ IDENTITY_CONTEXT	Nelze použít	MQZA_SET_ IDENTITY_CONTEXT **(“7” na stránce 163)**
MQOO_SET_ ALL_CONTEXT **(“5” na stránce 163, “8” na stránce 164)**	MQZAO_SET_ ALL_CONTEXT	Nelze použít	MQZA_SET_ ALL_CONTEXT **(“7” na stránce 163)**
MQOO_OUTPUT (Přenosová fronta) **(“9” na stránce 164)**	MQZAO_SET_ ALL_CONTEXT	Nelze použít	MQZA_SET_ ALL_CONTEXT **(“7” na stránce 163)**
MQOOK_SADA	MQZAO_SADA	Nelze použít	Žádná kontrola
MQO_ALTERNATE_ USER_AUTHORITY	**(“10” na stránce 164)**	**(“10” na stránce 164)**	MQZAO_ALTERNATE_ USER_AUTHORITY **(“10” na stránce 164, “11” na stránce 164)**

Tabulka 21. Autorizace zabezpečení potřebná pro volání MQPUT1			
Je vyžadována autorizace pro:	**Objekt fronty ("1" na stránce 163)**	**Objekt procesu**	**Objekt správce front**
KONTEXT MQPMO_PASS_ IDENTITY_CONTEXT	MQZA_PASS_ IDENTITY_CONTEXT **("12" na stránce 164)**	Nelze použít	Žádná kontrola
MQPMO_PASS_ALL _CONTEXT	MQZA_PASS_ ALL_CONTEXT **("12" na stránce 164)**	Nelze použít	Žádná kontrola
KONTEXT MQPMO_SET_ IDENTITY_CONTEXT	MQZA_SET_ IDENTITY_CONTEXT **("12" na stránce 164)**	Nelze použít	MQZA_SET_ IDENTITY_CONTEXT **("7" na stránce 163)**
MQPMO_SET_ ALL_CONTEXT	MQZA_SET_ ALL_CONTEXT **("12" na stránce 164)**	Nelze použít	MQZA_SET_ ALL_CONTEXT **("7" na stránce 163)**
(Přenosová fronta) **("9" na stránce 164)**	MQZAO_SET_ ALL_CONTEXT	Nelze použít	MQZA_SET_ ALL_CONTEXT **("7" na stránce 163)**
MQPMO_ALTERNATE_ USER_AUTHORITY	**("13" na stránce 164)**	Nelze použít	MQZAO_ALTERNATE_ USER_AUTHORITY **("11" na stránce 164)**

Tabulka 22. Autorizace zabezpečení potřebná pro volání MQCLOSE			
Je vyžadována autorizace pro:	**Objekt fronty ("1" na stránce 163)**	**Objekt procesu**	**Objekt správce front**
MQCO_DELETE	MQZAO_DELETE **("14" na stránce 164)**	Nelze použít	Nelze použít
VYPRÁZDNIT ODSTRANĚNÍ MQCO_DELETE	MQZAO_DELETE **("14" na stránce 164)**	Nelze použít	Nelze použít

Poznámky k tabulkám:

1. Otevírá-li se modelová fronta:
   - Pro modelovou frontu je zapotřebí oprávnění MQZAO_DISPLAY, kromě oprávnění k otevření modelové fronty pro typ přístupu, pro který se otevíráte.
   - Oprávnění MQZAO_CREATE není k vytvoření dynamické fronty zapotřebí.
   - Identifikátor uživatele použitý k otevření modelové fronty má automaticky udělena všechna oprávnění specifická pro danou frontu (ekvivalent MQZAO_ALL) pro vytvořenou dynamickou frontu.
2. Objekt správce front, proces, seznam názvů nebo objekt správce front je kontrolován v závislosti na typu otevíraný objektu.
3. Musí být zadán také parametr 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 164.
5. Musí být zadán také parametr MQOO_OUTPUT.
6. Tuto volbu má také implikovaná hodnota MQO_P_PASS_IDENTITY_CONTEXT.
7. Toto oprávnění je povinné jak pro objekt správce front, tak pro konkrétní frontu.

8. Tato volba předpokládá také MQOO_PASS_IDENTITY_CONTEXT, MQOO_PASS_ALL_CONTEXT a MQOO_SET_IDENTITY_CONTEXT.
9. Tato kontrola se provádí pro lokální nebo modelovou frontu, která má atribut fronty *Usage* MQUS_TRANSMISSION, a je otevírány přímo pro výstup. Nepoužije se, je-li otevřena vzdálená fronta (buď určením názvů vzdáleného správce front a vzdálené fronty, nebo zadáním názvu lokální definice vzdálené fronty).
10. Musí být zadán také alespoň jeden z příkazů MQOO_INQUIRE (pro každý typ objektu) nebo MQO_BROWSE, MQOO_INPUT_ *, MQOO_OUTPUT nebo MQOO_SET. U provedených kontrol je k dispozici kontrola ostatních voleb s použitím dodaného alternativního identifikátoru uživatele pro specifické oprávnění k objektu a aktuálního oprávnění aplikace pro kontrolu MQZAALTERNATE_USER_IDENTIFIER.
11. Toto oprávnění umožňuje zadat jakékoli *AlternateUserId* .
12. Kontrola MQZAO_OUTPUT se provádí také tehdy, pokud fronta nemá atribut fronty *Usage* MQUS_TRANSMISION.
13. U provedených kontrol se používají další zadané volby za použití poskytnutého alternativního identifikátoru uživatele pro uvedené oprávnění fronty a aktuální oprávnění aplikace pro kontrolu MQZAALTERNATE_USER_IDENTIFIER MQZAO_ALTERNATE_USER_IDENTIFIER.
14. Kontrola se provádí pouze v případě, že jsou splněny obě následující podmínky:
    - Trvalá dynamická fronta se zavírá a odstraňuje.
    - Fronta nebyla vytvořena pomocí operace MQOPEN, která vrátila použitou obsluhu objektu.

    Jinak žádná kontrola neexistuje.

Obecné poznámky:

1. Speciální autorizace MQZAO_ALL_MQI obsahuje všechny následující autorizace, které jsou relevantní pro daný typ objektu:
   - MQZAO_PŘIPOJENÍ
   - MQZAO_DOTÁZAT SE
   - MQZAO_SADA
   - MQZAO_BROWSE
   - MQZAO_VSTUP
   - MQZAO_VÝSTUP
   - KONTEXT MQZAO_PASS_IDENTITY_CONTEXT
   - MQZAO_PASS_ALL_CONTEXT
   - KONTEXT MQZAO_SET_IDENTITY_CONTEXT
   - FUNKCE MQZAO_SET_ALL_CONTEXT
   - MQZAO_ALTERNATE_USER_AUTHORITY
2. MQZAO_DELETE (viz poznámka “14” na stránce 164) a MQZAO_DISPLAY jsou klasifikovány jako autorizace pro administraci. Nejsou proto zahrnuty do struktury MQZAO_ALL_MQI.
3. *Žádná kontrola* znamená, že není prováděna žádná kontrola autorizace.
4. *Nepoužije se* znamená, že kontrola autorizace není pro tuto operaci relevantní. Například nemůžete vydat volání MQPUT pro objekt procesu.

IBM i *Oprávnění pro příkazy MQSC v řídicích PCF na serveru IBM i*

Tato oprávnění umožňují uživateli zadávat příkazy administrace jako řídicí dokument PCF. Tyto metody umožňují programu odeslat administrační příkaz jako zprávu správci front za účelem jeho provedení jménem tohoto uživatele.

Tato sekce shrnuje oprávnění potřebná pro každý příkaz MQSC obsažený v Escape PCF.

Nepoužije se znamená, že kontrola autorizace není pro tuto operaci relevantní.

ID uživatele, pod kterým je spuštěn program, který spouští příkaz, musí mít také následující oprávnění:

- Oprávnění MQZAO_CONNECT pro správce front
- Oprávnění DISPLAY pro správce front za účelem provedení příkazu PCF
- Oprávnění k vydávání příkazů MQSC v textu příkazu Escape PCF

ALTER *objekt*

Objekt	**Je vyžadována autorizace**
Fronta	ZMĚNA MQZAO_CHANGE
Téma	ZMĚNA MQZAO_CHANGE
Proces	ZMĚNA MQZAO_CHANGE
Správce front	ZMĚNA MQZAO_CHANGE
Seznam názvů	ZMĚNA MQZAO_CHANGE
Ověřovací informace	ZMĚNA MQZAO_CHANGE
Kanál	ZMĚNA MQZAO_CHANGE
Kanál připojení klienta	ZMĚNA MQZAO_CHANGE
Modul listener	ZMĚNA MQZAO_CHANGE
Služba	ZMĚNA 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 168)

Objekt	**Je vyžadována autorizace**
Fronta	MQZAO_CREATE **(“2” na stránce 169)**
Téma	MQZAO_CREATE **(“2” na stránce 169)**
Proces	MQZAO_CREATE **(“2” na stránce 169)**
Správce front	Nelze použít
Seznam názvů	MQZAO_CREATE **(“2” na stránce 169)**
Ověřovací informace	MQZAO_CREATE **(“2” na stránce 169)**

Objekt	Je vyžadována autorizace
Kanál	MQZAO_CREATE **(“2” na stránce 169)**
Kanál připojení klienta	MQZAO_CREATE **(“2” na stránce 169)**
Modul listener	MQZAO_CREATE **(“2” na stránce 169)**
Služba	MQZAO_CREATE **(“2” na stránce 169)**

DEFINE *objekt* REPLACE (“1” na stránce 168, “3” na stránce 169)

Objekt	Je vyžadována autorizace
Fronta	ZMĚNA MQZAO_CHANGE
Téma	ZMĚNA MQZAO_CHANGE
Proces	ZMĚNA MQZAO_CHANGE
Správce front	Nelze použít
Seznam názvů	ZMĚNA MQZAO_CHANGE
Ověřovací informace	ZMĚNA MQZAO_CHANGE
Kanál	ZMĚNA MQZAO_CHANGE
Kanál připojení klienta	ZMĚNA MQZAO_CHANGE
Modul listener	ZMĚNA MQZAO_CHANGE
Služba	ZMĚNA 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
Služba	MQZAO_DELETE

DISPLAY *objekt*

Objekt	Je vyžadována autorizace
Fronta	MQZAO_ZOBRAZENÍ
Téma	MQZAO_ZOBRAZENÍ
Proces	MQZAO_ZOBRAZENÍ
Správce front	MQZAO_ZOBRAZENÍ

Objekt	Je vyžadována autorizace
Seznam názvů	MQZAO_ZOBRAZENÍ
Ověřovací informace	MQZAO_ZOBRAZENÍ
Kanál	MQZAO_ZOBRAZENÍ
Kanál připojení klienta	MQZAO_ZOBRAZENÍ
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
Kanál připojení klienta	Nelze použít
Modul listener	Nelze použít
Služba	Nelze použít

Vyřešit kanál

Objekt	Je vyžadována autorizace
Fronta	Nelze použít
Téma	Nelze použít

Objekt	Je vyžadována autorizace
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
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 pro objekt LIKE také zapotřebí oprávnění MQZAO_DISPLAY, je-li zadán, nebo na příslušném SYSTEM.DEFAULT.xxx , je-li LIKE vynechán.

2. Oprávnění CREATE MQZAO_CREATE není specifické pro konkrétní objekt nebo typ objektu. Oprávnění k vytvoření je uděleno pro všechny objekty pro určitého správce front uvedením 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 určena pro atribut DEFINE *object* NOREPLACE.

IBM i *Oprávnění pro příkazy PCF na systému IBM i*

Tato oprávnění umožňují uživateli zadávat příkazy administrace jako příkazy PCF. Tyto metody umožňují programu odeslat administrační příkaz jako zprávu správci front za účelem jeho provedení jménem tohoto uživatele.

Tato sekce shrnuje oprávnění potřebná pro každý příkaz PCF.

Žádná kontrola znamená, že není prováděna žádná kontrola autorizace; *Nepoužije se* znamená, že kontrola autorizace není pro tuto operaci relevantní.

ID uživatele, pod kterým je spuštěn program, který spouští příkaz, musí mít také následující oprávnění:

- Oprávnění MQZAO_CONNECT pro správce front
- Oprávnění DISPLAY pro správce front za účelem provedení příkazu PCF

Speciální autorizace MQZAO_ALL_ADMIN zahrnuje následující autorizace:

- ZMĚNA MQZAO_CHANGE
- MQZAO_CLEAR
- MQZAO_DELETE
- MQZAO_ZOBRAZENÍ
- MQZAO_CONTROL
- MQZAO_CONTROL_EXTENDED

Objekt MQZAO_CREATE není zahrnut, protože není specifický pro konkrétní objekt nebo typ objektu.

Změna *objektu*

Objekt	**Je vyžadována autorizace**
Fronta	ZMĚNA MQZAO_CHANGE
Téma	ZMĚNA MQZAO_CHANGE
Proces	ZMĚNA MQZAO_CHANGE
Správce front	ZMĚNA MQZAO_CHANGE
Seznam názvů	ZMĚNA MQZAO_CHANGE
Ověřovací informace	ZMĚNA MQZAO_CHANGE
Kanál	ZMĚNA MQZAO_CHANGE
Kanál připojení klienta	ZMĚNA MQZAO_CHANGE
Modul listener	ZMĚNA MQZAO_CHANGE
Služba	ZMĚNA MQZAO_CHANGE

Vymazat *objekt*

Objekt	**Je vyžadována autorizace**
Fronta	MQZAO_CLEAR
Téma	MQZAO_CLEAR

Objekt	Je vyžadována autorizace
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

Kopírování *objektu* (bez náhrady) (“1” na stránce 174)

Objekt	Je vyžadována autorizace
Fronta	MQZAO_CREATE **(“2” na stránce 174)**
Téma	MQZAO_CREATE **(“2” na stránce 174)**
Proces	MQZAO_CREATE **(“2” na stránce 174)**
Správce front	Nelze použít
NamelistMQZAO_VYTVOŘENÍ	MQZAO_CREATE **(“2” na stránce 174)**
Ověřovací informace	MQZAO_CREATE **(“2” na stránce 174)**
Kanál	MQZAO_CREATE **(“2” na stránce 174)**
Kanál připojení klienta	MQZAO_CREATE **(“2” na stránce 174)**
Modul listener	MQZAO_CREATE **(“2” na stránce 174)**
Služba	MQZAO_CREATE **(“2” na stránce 174)**

Kopírování *objektu* (s nahrazením) (“1” na stránce 174, “4” na stránce 175)

Objekt	Je vyžadována autorizace
Fronta	ZMĚNA MQZAO_CHANGE
Téma	ZMĚNA MQZAO_CHANGE
Proces	ZMĚNA MQZAO_CHANGE
Správce front	Nelze použít
Seznam názvů	ZMĚNA MQZAO_CHANGE
Ověřovací informace	ZMĚNA MQZAO_CHANGE
Kanál	ZMĚNA MQZAO_CHANGE
Kanál připojení klienta	ZMĚNA MQZAO_CHANGE
Modul listener	ZMĚNA MQZAO_CHANGE
Služba	ZMĚNA MQZAO_CHANGE

Vytvořit *objekt* (bez náhrady) (“3” na stránce 174)

Objekt	Je vyžadována autorizace
Fronta	MQZAO_CREATE **(“2” na stránce 174)**
Téma	MQZAO_CREATE **(“2” na stránce 174)**
Proces	MQZAO_CREATE **(“2” na stránce 174)**
Správce front	Nelze použít
Seznam názvů	MQZAO_CREATE **(“2” na stránce 174)**
Ověřovací informace	MQZAO_CREATE **(“2” na stránce 174)**
Kanál	MQZAO_CREATE **(“2” na stránce 174)**
Kanál připojení klienta	MQZAO_CREATE **(“2” na stránce 174)**
Modul listener	ZMĚNA MQZAO_CHANGE
Služba	ZMĚNA MQZAO_CHANGE

Vytvořit *objekt* (s nahrazením) (“3” na stránce 174, “4” na stránce 175)

Objekt	Je vyžadována autorizace
Fronta	ZMĚNA MQZAO_CHANGE
Téma	ZMĚNA MQZAO_CHANGE
Proces	ZMĚNA MQZAO_CHANGE
Správce front	Nelze použít
Seznam názvů	ZMĚNA MQZAO_CHANGE
Ověřovací informace	ZMĚNA MQZAO_CHANGE
Kanál	ZMĚNA MQZAO_CHANGE
Kanál připojení klienta	ZMĚNA MQZAO_CHANGE
Modul listener	ZMĚNA MQZAO_CHANGE
Služba	ZMĚNA MQZAO_CHANGE

Odstranit *objekt*

Objekt	Je vyžadována autorizace
Fronta	MQZAO_DELETE
Téma	MQZAO_DELETE
Proces	MQZAO_DELETE
Správce front	MQZAO_DELETE
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

Zjišťovat *objekt*

Objekt	Je vyžadována autorizace
Fronta	MQZAO_ZOBRAZENÍ
Téma	MQZAO_ZOBRAZENÍ
Proces	MQZAO_ZOBRAZENÍ
Správce front	MQZAO_ZOBRAZENÍ
Seznam názvů	MQZAO_ZOBRAZENÍ
Ověřovací informace	MQZAO_ZOBRAZENÍ
Kanál	MQZAO_ZOBRAZENÍ
Kanál připojení klienta	MQZAO_ZOBRAZENÍ
Modul listener	MQZAO_ZOBRAZENÍ
Služba	MQZAO_ZOBRAZENÍ

Zjišťovat názvy *objektů*

Objekt	Je vyžadována autorizace
Fronta	Žádná kontrola
Téma	Žádná kontrola
Proces	Žádná kontrola
Správce front	Žádná kontrola
Seznam názvů	Žádná kontrola
Ověřovací informace	Žádná kontrola
Kanál	Žádná kontrola
Kanál připojení klienta	Žádná kontrola
Modul listener	Žádná kontrola
Služba	Žádná kontrola

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

Objekt	Je vyžadována autorizace
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	Funkce 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

Objekt	Je vyžadována autorizace
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
Služba	Nelze použít

Poznámka:

1. Pro příkazy Kopírovat je oprávnění MQZAO_DISPLAY také potřebné pro objekt From.
2. Oprávnění CREATE MQZAO_CREATE není specifické pro konkrétní objekt nebo typ objektu. Oprávnění k vytvoření je uděleno pro všechny objekty pro určitého správce front uvedením typu objektu QMGR v příkazu GRTMQMAUT .
3. Pro příkazy Create je zapotřebí oprávnění MQZAO_DISPLAY také pro příslušný SYSTEM.DEFAULT.* objekt.

4. Tato volba se použije, pokud objekt, který má být nahrazen, již existuje. Pokud tomu tak není, je kontrola funkce Kopírovat nebo Vytvořit bez náhrady.

IBM i Generické profily OAM v systému IBM i

Generické profily správce oprávnění k objektu (OAM) vám umožňují nastavit oprávnění, které má uživatel k mnoha objektům najednou, místo toho, abyste museli vydávat samostatné příkazy **GRTMQMAUT** pro každý jednotlivý objekt, když je vytvářen. Použití generických profilů v příkazu **GRTMQMAUT** vám umožňuje nastavit generické oprávnění pro všechny budoucí vytvořené objekty, které jsou vhodné pro daný profil.

Zbývající část tohoto oddílu popisuje použití generických profilů podrobněji:

- "Použití zástupných znaků" na stránce 175
- "Priority profilu" na stránce 175

Použití zástupných znaků

Co znamená, že generický profil je použití speciálních znaků (zástupné znaky) v názvu profilu. Zástupný znak otazníku (?) se například shoduje s libovolným znakem v názvu. Pokud tedy zadáte `ABC.?EF`, autorizace, kterou poskytnete tomuto profilu, se vztahuje na všechny objekty vytvořené s názvy `ABC.DEF`, `ABC.CEF`, `ABC.BEF`atd.

Dostupné zástupné znaky jsou:

?

Otazník (?) zastupuje libovolný jeden znak. Například `AB.?D` by se vztahovala na objekty `AB.CD`, `AB.EDa AB.FD`.

*****

Použijte hvězdičku (*) jako:

- *Kvalifikátor* v názvu profilu, který odpovídá 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 vztahovala na objekty `ABC.DEF.JKLa ABC.GHI.JKL`. (Všimněte si, že by se **nevztahovalo** na `ABC.JKL` ; * použitý v tomto kontextu vždy označuje jeden kvalifikátor.)
- Znak uvnitř kvalifikátoru v názvu profilu, který odpovídá žádnému znaku nebo více znakům v rámci kvalifikátoru ve jménu objektu.

  Například `ABC.DE*.JKL` by se vztahovala na objekty `ABC.DE.JKL`, `ABC.DEF.JKLa ABC.DEGH.JKL`.

******

Použijte dvojité hvězdičky (**) ***jednou*** v názvu profilu jako:

- Celý název profilu, který odpovídá všem názvům objektů. Pokud například použijete klíčové slovo `OBJTYPE (*PRC)` k identifikaci procesů, pak jako název profilu použijte ** **, změníte oprávnění pro všechny procesy.
- Jako počáteční, střední nebo koncový kvalifikátor v názvu profilu odpovídá jednomu nebo více kvalifikátorům v názvu objektu. Například, `**.ABC` identifikuje všechny objekty s konečným kvalifikátorem ABC.

Priority profilu

Důležitým bodem pro pochopení použití generických profilů je priorita, která jsou při rozhodování o tom, jaká oprávnění mají být použita na vytvářený objekt, upřednostňována. Předpokládejme například, že jste tyto příkazy zadali:

```
GRTMQMAUT OBJ(AB.*) OBJTYPE(*Q) USER(FRED) AUT(*PUT) MQMNAME(MYQMGR)
GRTMQMAUT OBJ(AB.C*) OBJTYPE(*Q) USER(FRED) AUT(*GET) MQMNAME(MYQMGR)
```

První dává oprávnění ke všem frontám pro činitele FRED s názvy, které odpovídají profilu AB. *; druhý dává oprávnění ke stejným typům front, které odpovídají profilu AB.C*.

Předpokládejme, že nyní vytvoříte frontu s názvem AB.CD. Podle pravidel pro shodu se zástupnými znaky může být GRTMQMAUT použit pro tuto frontu. Takže, má to dát nebo získat oprávnění?

Chcete-li najít odpověď, aplikujete pravidlo, které, kdykoli se může na objekt použít více profilů, **pouze nejspecifičtější použití**. Způsob použití tohoto pravidla je porovnáváním názvů profilů zleva doprava. Kdekoli se liší, negenerický znak je specifičtější než generický znak. Takže, v předchozím příkladu, fronta AB.CD má autoritu **get** (AB.C* je více specifická než AB. *).

Porovnáváte-li generické znaky, pořadí *specifičnosti* je:

1. ?
2. *
3. **

IBM i Uvedení instalované autorizační služby na IBM i

Můžete uvést, která komponenta autorizační služby se má použít.

Parametr **Service Component name** na **GRTMQMAUT** a **RVKMQMAUT** vám umožňuje uvést název instalované komponenty autorizační služby.

Výběr volby **F24** na počátečním panelu, za nímž následuje příkaz **F9=All** na dalším panelu příkazu, umožňuje zadat buď instalovanou autorizační komponentu (*DFT), nebo název požadované komponenty autorizační služby určené ve stanze Service v souboru qm.ini správce front.

DSPMQMAUT má také tento parametr navíc. Tento parametr vám umožňuje prohledat všechny nainstalované autorizační komponenty (*DFT), nebo zadané jméno komponenty autorizační služby, pro uvedený název objektu, typ objektu a uživatele

IBM i Práce s profily oprávnění a bez nich na serveru IBM i

V této části se dozvíte, jak pracovat s profily oprávnění a jak pracovat bez profilů oprávnění.

Můžete pracovat s profily oprávnění, jak je vysvětleno v publikaci “Práce s profily oprávnění” na stránce 176, nebo bez nich, jak je vysvětleno zde:

Chcete-li pracovat bez profilů oprávnění, použijte *NONE jako parametr oprávnění na **GRTMQMAUT** , abyste vytvořili profily bez oprávnění. To ponechá všechny existující profily nezměněné.

V systému **RVKMQMAUT**použijte jako parametr oprávnění *REMOVE k odebrání existujícího profilu oprávnění.

Práce s profily oprávnění

K profilování oprávnění jsou přidruženy dva příkazy:

- **WRKMQMAUT**
- **WRKMQMAUTD**

K těmto příkazům můžete přistoupit přímo z příkazového řádku nebo z panelu WRKMQM podle:

1. Zadání názvu správce front a stisknutí klávesy Enter pro přístup k panelu výsledků produktu **WRKMQM** .
2. Vyberte volbu F23=More options na tomto panelu.

Volba 24 vybere panel s výsledky pro příkaz **WRKMQMAUT** a volba 25 vybere příkaz **WRKMQMAUTI** , který se používá ve vrstvě 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 tisknete informace na obrazovku, zobrazí se seznam názvů profilů oprávnění spolu s jejich typy. Pokud tisknete výstup, obdržíte podrobný seznam všech dat oprávnění, registrovaných uživatelů a jejich oprávnění.

Na tomto panelu zadejte název objektu nebo profilu a stisknutím klávesy Enter přejdete na panel výsledků pro produkt **WRKMQMAUT** .

Vyberete-li volbu `4=Delete`, přejdete na nový panel, ze kterého můžete potvrdit, že chcete odstranit všechny názvy uživatelů zaregistrované na generický název profilu oprávnění, který jste zadali. Tato volba spustí **RVKMQMAUT** s volbou *REMOVE pro všechny uživatele a použije **pouze** pro generické názvy profilů.

Vyberete-li volbu `12=Work with profile` , přejdete na panel s výsledky příkazu **WRKMQMAUTD** , jak je vysvětleno v části “WRKMQMAUTD” na stránce 177.

WRKMQMAUTD

Tento příkaz umožňuje zobrazit všechny uživatele registrované s určitým 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, který potřebujete, oprávnění QMQMADM.

Výběrem volby `F24=More keys` z počátečního vstupního panelu následovaným volbou `F9=All Parameters` se zobrazí název komponenty služby jako pro **GRTMQMAUT** a **RVKMQMAUT**.

Poznámka: Klávesa `F11=Display Object Authorizations` se přepíná mezi následujícími typy oprávnění:

- Oprávnění k objektu
- Kontextové autorizace
- Autorizace MQI

Volby na obrazovce jsou:

2=Grant
Vezme vás na panel **GRTMQMAUT** , abyste jej přidali do aktuálních oprávnění.

3=Revoke
Vezme 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. To spustí **RVKMQMAUT** s volbou *REMOVE.

5=Display
Vezme vás na existující příkaz **DSPMQMAUT**

F6=Create
Přenese vás na panel **GRTMQMAUT** , který vám umožňuje vytvořit záznam oprávnění 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 Přehled MQMD.

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 “Ověřování kanálu” na stránce 108.

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 v 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 produkt RACF.

Související odkazy

Scénář zabezpečení: dva správci front v systému z/OS

Scénář zabezpečení: skupina sdílení front v systému z/OS

z/OS Třídy zabezpečení produktu RACF

Třídy RACF se používají k uchování profilů požadovaných pro kontrolu zabezpečení produktu IBM MQ . Řada z tříd členů má ekvivalentní třídy skupin. Musíte aktivovat třídy a povolit jim přijetí generických profilů.

Každá třída RACF obsahuje jeden nebo více profilů použitých v určitém bodě v kontrolní posloupnosti, jak je zobrazeno v části Tabulka 23 na stránce 180.

Tabulka 23. Třídy RACF použité produktem IBM MQ

Třída členů	Třída skupiny	Obsah
MQADMIN	GMQADMIN	Profily, které se používají hlavně pro administrativní funkce. Příklad: • Profily pro přepínače zabezpečení produktu IBM MQ . • Profil zabezpečení RESLEVEL. • Profily pro alternativní zabezpečení uživatelů. • Profily pro zabezpečení kontextu. • Profily pro zabezpečení prostředků příkazů. Tato třída může obsahovat pouze velké profily RACF .
MXADMIN	GMXADMIN	Profily, které se používají hlavně pro administrativní funkce. Příklad: • Profily pro přepínače zabezpečení produktu IBM MQ . • Profil zabezpečení RESLEVEL. • Profily pro alternativní zabezpečení uživatelů. • Profily pro zabezpečení kontextu. • Profily pro zabezpečení prostředků příkazů. Tato třída může obsahovat jak velké, tak i profily s kombinovaným profilem RACF .
MQCONN		Profily použité pro zabezpečení připojení.
MQCMDS		Profily použité pro zabezpečení příkazů.
MQQUEUE	FRONTA GMQQUEUE	Profily ve frontě použité ve zabezpečení prostředků fronty.
MXQUEUE	GMXQUEUE	Kombinované profily s velkými písmeny a velkými písmeny použité ve zabezpečení prostředků fronty.
MQPROC	GMQPROC	Velké profily používané v zabezpečení prostředků procesu.
MXPROC	GMXPROC	Kombinované profily s velkými a velkými písmeny použité v zabezpečení prostředků procesu.
MQNLIST	SEZNAM GMQNLIST	Profily ve velké velikosti použité v zabezpečení prostředků seznamu názvů.
MXNLIST	GMXNLIST	V zabezpečení prostředků seznamu názvů se používají profily se smíšenou velikostí písmen a velkými písmeny.

Tabulka 23. Třídy RACF použité produktem IBM MQ (pokračování)		
Třída členů	**Třída skupiny**	**Obsah**
MXTOPIC	GMXTOPIC	Kombinované profily a profily velkých a malých písmen použité v zabezpečení témat.

Některé třídy mají související *třídu skupiny* , která vám umožňuje dát dohromady skupiny prostředků s podobnými požadavky na přístup. Podrobnosti o rozdílu mezi členskou a skupinovou třídou a při použití členu nebo třídy skupiny naleznete v příručce z/OS Security Server RACF Security Administrator's Guide.

Třídy musí být aktivovány před tím, než mohou být provedeny kontroly 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 také zajistit, abyste nastavili třídy tak, aby mohly přijímat generické profily. Toto můžete provést 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 produktu RACF použité produktem IBM MQ obsahují předponu, což je buď název správce front, nebo název skupiny sdílení front. Při použití znaku procenta jako zástupného znaku buďte opatrní.

Všechny profily produktu RACF použité produktem IBM MQ obsahují předponu. Pro zabezpečení na úrovni skupiny sdílení front se jedná o název skupiny sdílení front. Pro úroveň zabezpečení správce front je předponou název správce front. Používáte-li směs správce front a zabezpečení na úrovni skupiny sdílení front, budete používat profily s oběma typy předpony. Úroveň zabezpečení skupiny sdílení front a správce front je popsána v tématu Ovládací prvky zabezpečení a volby 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 jako RACF jako:

```
RDEFINE MQQUEUE QSG1.QUEUE_FOR_SUBSCRIBER_LIST
```

Chcete-li chránit frontu s názvem QUEUE_FOR_LOST_CARD_LIST, která náleží do správce front STCD na úrovni správce front, bude příslušný profil definován jako RACF jako:

```
RDEFINE MQQUEUE STCD.QUEUE_FOR_LOST_CARD_LIST
```

To znamená, že různí správci front a skupiny sdílení front mohou sdílet stejnou databázi RACF a mají však různé možnosti zabezpečení.

Nepoužívejte generické názvy správce front v profilech, abyste se vyhnuli nepředpokládanému přístupu uživatelů.

IBM MQ umožňuje použití znaku procenta (%) v názvech objektů. RACF však používá znak% jako zástupný znak s jedním znakem. To znamená, že když definujete jméno objektu se znakem% v jeho názvu, musíte to vzít v úvahu při definování odpovídajícího profilu.

For example, for the queue CREDIT_CARD_%_RATE_INQUIRY, on queue manager CRDP, the profile would be defined to RACF as follows:

```
RDEFINE MQQUEUE CRDP.CREDIT_CARD_%_RATE_INQUIRY
```

Tuto frontu nelze chránit generickým profilem, jako např. CRDP. * *.

IBM MQ umožňuje použití velkých a malých písmen v názvech objektů. Tyto objekty můžete chránit definováním:

1. kombiné profily případů v příslušných třídách RACF se smíšenými malými a velkými písmeny, nebo
2. Generické profily v příslušných velkých třídách RACF .

Chcete-li použít profily se smíšenými případy a smíšené třídy RACF , musíte postupovat podle kroků popsaných v tématu “Migrace správce front z/OS na smíšenou velikost písmen” na stránce 262.

Jsou zde některé profily nebo části profilů, které zůstávají velkými písmeny pouze v případě, že jsou hodnoty poskytnuty produktem IBM MQ. Patří mezi ně:

- Přepnout profily.
- Všechny kvalifikátory vysoké úrovně (HLQ) včetně subsystémů a identifikátorů 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.
- Profily produktu **RESLEVEL** .
- Kvalifikace produktu `'object'` v profilech prostředků příkazu; například `hlq.QUEUE.queuename`. Název prostředku je pouze malá a velká písmena.
- Dynamické profily front `hlq.CSQOREXX.*`, `hlq.CSQUTIL.*`a `CSQXCMD.*`.
- Část `'CONTEXT'` části `hlq.CONTEXT.resourcename`.
- Část `'ALTERNATE.USER'` části `hlq.ALTERNATE.USER.userid`.

Můžete například definovat profil pro udělení přístupu k 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 velké profily, můžete definovat profil ve třídě IBM MQ RACF `MQQUEUE` pomocí následujícího příkazu:

  ```
  RDEFINE MQQUEUE MQ01.PAYROLL.*
  ```

První příklad použití profilů smíšených případů vám poskytuje přesnější kontrolu nad udělením oprávnění pro přístup k prostředku.

z/OS Profily přepínače

Chcete-li řídit kontrolu zabezpečení provedenou produktem IBM MQ, použijte *profily přepínače*. Profil přepínače je normální profil RACF , který má speciální význam pro IBM MQ. Seznam pro přístup v profilech přepínačů není používán produktem IBM MQ.

Produkt IBM MQ udržuje interní přepínač pro každý typ přepínače zobrazený v tabulkách Přepnout profily pro zabezpečení na úrovni subsystému, Přepnout profily pro skupinu sdílení front nebo zabezpečení na úrovni správce fronta Přepnout profily pro kontrolu prostředků. Profily přepínače lze udržovat na úrovni

skupiny sdílení front nebo na úrovni správce front, nebo v kombinaci obou. Pomocí jediné sady profilů přepínače zabezpečení skupiny sdílení front můžete řídit zabezpečení všech správců front v rámci skupiny sdílení front.

Je-li nastaven přepínač zabezpečení, provedou se kontroly zabezpečení přidružené k přepínači. Je-li přepínač zabezpečení vypnut, bezpečnostní kontroly přidružené k přepínači budou vynechány. Předvolba 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 produktu RACF .

Když je správce front spuštěn (nebo když je třída MQADMIN nebo MXADMIN obnovena příkazem IBM MQ REFRESH SECURITY), produkt IBM MQ nejprve zkontroluje stav RACF a příslušné třídy:

- Třída MQADMIN, používáte-li velké profily
- Třída MXADMIN, používáte-li smíšený profil případu.

Je-li některá z těchto podmínek pravdivá, nastaví přepínač zabezpečení subsystému:

- RACF je neaktivní nebo není instalovaný.
- Třída MQADMIN nebo MXADMIN není definována (tyto třídy jsou vždy definovány pro RACF , protože jsou zahrnuty v tabulce deskriptorů třídy (CDT)).
- Třída MQADMIN nebo MXADMIN nebyla aktivována.

Je-li třída RACF i třída MQADMIN nebo MXADMIN aktivní, produkt IBM MQ zkontroluje třídu MQADMIN nebo MXADMIN, aby zjistil, zda některý z profilů přepínačů nebyl definován. Nejprve zkontroluje profily popsané v části “Profily pro řízení zabezpečení subsystému” na stránce 184. Není-li zabezpečení subsystému vyžadováno, IBM MQ nastaví zabezpečení interního 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 nastaven některý z přepínačů IBM MQ , program IBM MQ zkontroluje stav třídy RACF přidružené k typu zabezpečení, který odpovídá přepínači IBM MQ . Není-li třída nainstalována nebo není aktivní, je přepínač IBM MQ vypnut. Kontroly zabezpečení procesů se například neprovádějí, pokud nebyla aktivována třída MQPROC nebo MXPROC. Třída, která není aktivní, je ekvivalentní definování NO.PROCESS.CHECKS profil pro každého správce front a skupinu sdílení front, která používá tuto databázi RACF .

z/OS *Jak fungují přepínače*

Chcete-li nastavit přepínač zabezpečení, definujte hodnotu NO.*. Profil přepínače pro tento profil. NOV..* lze přepsat. profil nastavený na úrovni skupiny sdílení front definováním YES.* pro správce front.

Chcete-li nastavit přepínač zabezpečení, je třeba definovat hodnotu NO.*. Profil přepínače pro tento profil. Existence položky NO.* profil znamená, že kontroly zabezpečení **nejsou** prováděny pro daný typ prostředku, pokud se nerozhodnete přepsat nastavení úrovně skupiny sdílení front v konkrétním správci front. Tento popis je popsán v tématu “Přepsání nastavení úrovně skupiny sdílení front” na stránce 184.

Není-li váš správce front členem skupiny sdílení front, není třeba definovat žádné profily skupin sdílení front nebo žádné profily pro potlačení. Je však třeba tyto profily definovat, pokud správce front připojí skupinu sdílení front k pozdějšímu datu.

Každý NO.* Profil přepínače, který příkaz IBM MQ detekuje, vypíná kontrolu daného typu prostředku. Profily přepnutí se aktivují při spuštění správce front. Pokud změníte profily přepínače, zatímco jsou spuštěni všichni postižení správci front, můžete produkt IBM MQ získat, aby rozpoznal změny vydáním 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 Přepnutí profilů pro kontrolu prostředků zobrazují platné profily přepínače a typ zabezpečení, který řídí.

Přepsání nastavení úrovně skupiny sdílení front

Nastavení zabezpečení na úrovni skupiny sdílení front pro konkrétního správce front, který je členem této skupiny, lze potlačit. Chcete-li provést kontroly správce front v jednotlivých správcích front, které nejsou provedeny v jiných správcích front ve skupině, použijte příkaz (qmgr-name.YES. *) profily přepínačů.

A naopak, pokud nechcete provést určitou kontrolu u jednoho konkrétního správce front v rámci skupiny sdílení front, definujte soubor (qmgr-name.NO. *) profilu pro tento konkrétní typ prostředku ve správci front a nedefinujte profil pro skupinu sdílení front. (IBM MQ kontroluje pouze profil úrovně skupiny sdílení front, pokud nenalezne profil úrovně správce front.)

z/OS *Profily pro řízení zabezpečení subsystému*

Produkt IBM MQ kontroluje, zda jsou pro subsystém, pro správce front a pro skupinu sdílení front vyžadovány kontroly zabezpečení subsystému.

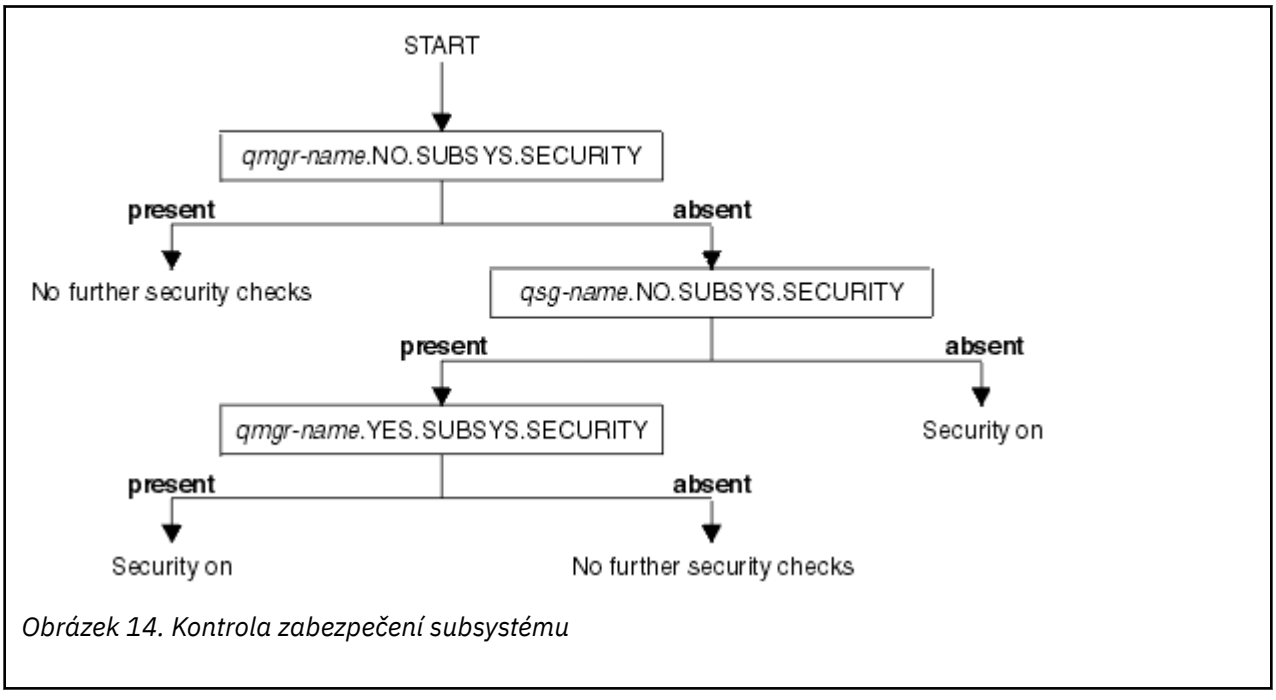
První kontrola zabezpečení provedená pomocí IBM MQ se používá k určení, zda jsou bezpečnostní kontroly vyžadovány pro celý subsystém IBM MQ . Pokud uvedete, že nechcete zabezpečení subsystému, nebudou provedeny žádné další kontroly.

Jsou zkontrolovány následující profily přepínače, aby se určilo, zda je zabezpečení subsystému povinné. Obrázek 14 na stránce 184 zobrazuje pořadí, ve kterém jsou zkontrolovány.

Tabulka 24. Přepnout profily pro zabezpečení na úrovni subsystému

Název profilu přepínače	**Typ prostředku nebo kontrolování, které je řízeno**
qmgr-name.NO.SUBSYS.SECURITY	Zabezpečení podsystému pro tohoto správce front
qsg-name.NO.SUBSYS.SECURITY	Zabezpečení podsystému 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, příkaz IBM MQ vyhledá pouze profil přepínače qmgr-name.NO.SUBSYS.SECURITY .



Obrázek 14. Kontrola zabezpečení subsystému

z/OS *Profily pro zabezpečení skupiny sdílení front nebo zabezpečení na úrovni správce front*

Je-li vyžadována kontrola zabezpečení subsystému, produkt IBM MQ kontroluje, zda je kontrola zabezpečení vyžadována ve skupině sdílení front nebo na úrovni správce front.

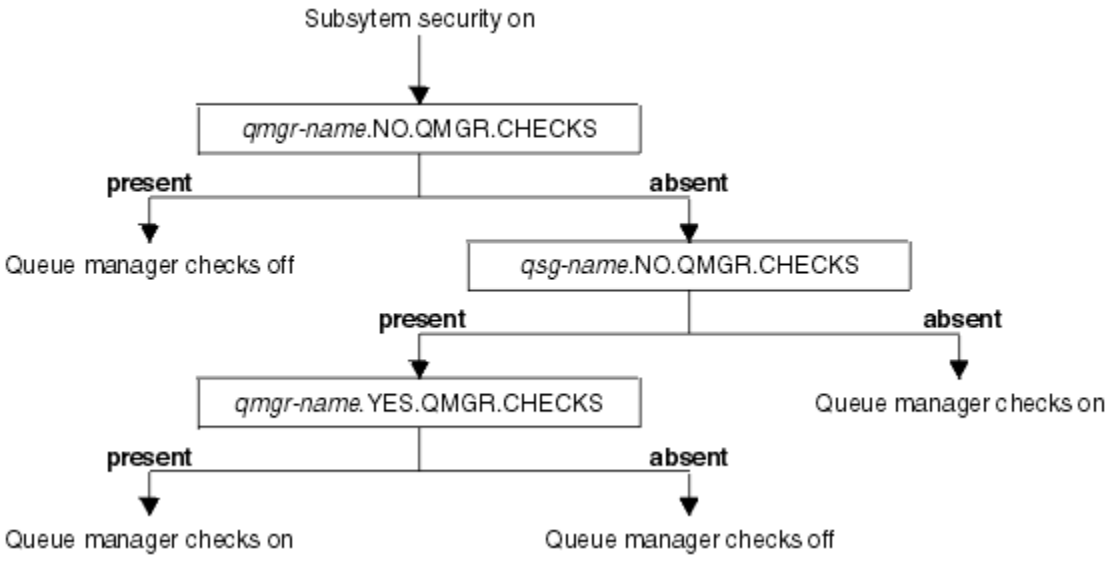
Když produkt IBM MQ určil, že je vyžadována kontrola zabezpečení, pak určuje, zda je vyžadována kontrola na úrovni skupiny sdílení front nebo správce front, nebo obojí. Tyto kontroly se neprovedou, pokud váš správce front není členem skupiny sdílení front.

Požadují se následující profily přepínačů, aby bylo možné určit požadovanou úroveň. Obrázek 15 na stránce 185 a Obrázek 16 na stránce 186 zobrazují pořadí, ve kterém jsou zaškrtnuty.

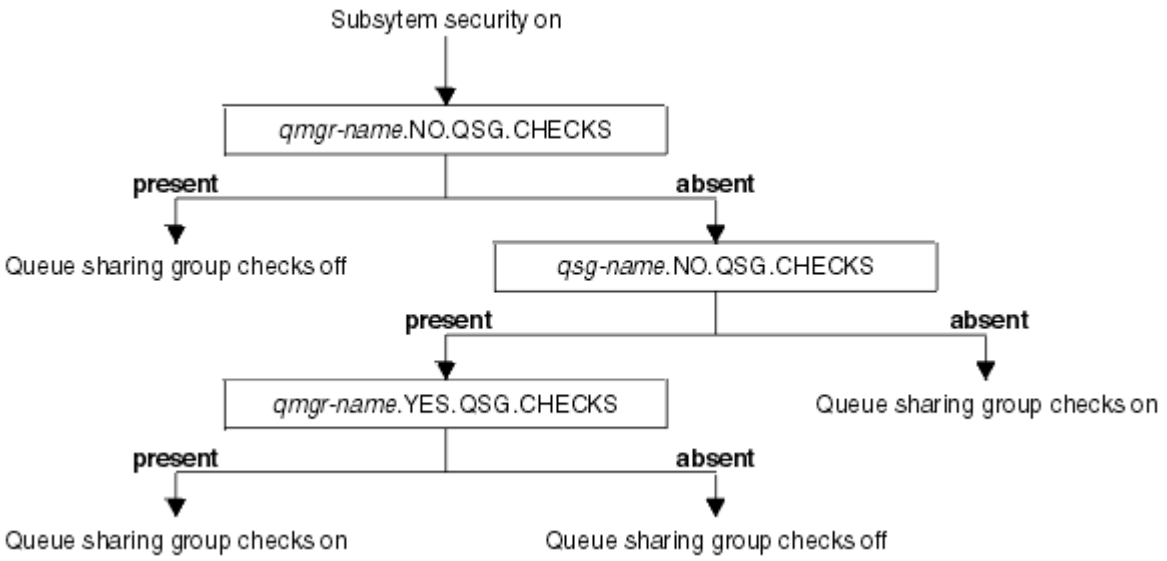
Tabulka 25. Přepnout profily pro skupinu sdílení front nebo zabezpečení na úrovni správce front

Název profilu přepínače	**Typ prostředku nebo kontrolování, které je řízeno**
qmgr-name.NO.QMGR.CHECKS	Žádné kontroly úrovně správce front pro tohoto správce front
qsg-name.NO.QMGR.CHECKS	Pro tuto skupinu sdílení front nejsou žádné kontroly na úrovni správce front.
qmgr-name.YES.QMGR.CHECKS	Přepsání kontroly úrovně správce front pro tohoto správce front
qmgr-name.NO.QSG.CHECKS	Žádné kontroly úrovně skupiny sdílení front pro tohoto správce front
qsg-name.NO.QSG.CHECKS	Žádná úroveň skupiny sdílení front pro tuto skupinu sdílení front nekontroluje
qmgr-name.YES.QSG.CHECKS	Potlačení úrovně skupiny sdílení front pro tohoto správce front

Je-li zabezpečení subsystému aktivní, nemůžete vypnout jak skupinu sdílení front, tak zabezpečení na úrovni správce front. Pokud se o to pokusíte, 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 přepínačů zabezpečení*

Platné jsou pouze některé kombinace přepínačů. Pokud použijete kombinaci nastavení přepínačů, která není platná, je vydána zpráva CSQH026I a kontrola zabezpečení je nastavena na úrovni skupiny sdílení front i na úrovni správce front.

Tabulka 26 na stránce 186, Tabulka 27 na stránce 186, Tabulka 28 na stránce 187a Tabulka 29 na stránce 187 zobrazují sady kombinací nastavení přepínačů, 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
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

Tabulka 27. Platné kombinace přepínačů zabezpečení pro zabezpečení na úrovni skupiny sdílení front (pokračování)
Kombinace
qsg-name.NO.QMGR.CHECKS qsg-name.NO.QSG.CHECKS qmgr-name.YES.QSG.CHECKS

Tabulka 28. Platné kombinace přepínačů zabezpečení pro správce front a zabezpečení na úrovni skupiny sdílení front
Kombinace
qsg-name.NO.QMGR.CHECKS qmgr-name.YES.QMGR.CHECKS Ne QSG.* definované profily
Žádný 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 definovaný přepínač

*Tabulka 29. Další platné kombinace přepínačů zabezpečení, které přepínají obě úrovně kontroly **zapnu**.*
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 na úrovni prostředků*

K řízení přístupu k prostředkům se používá řada profilů přepínačů. U správce front nebo skupiny sdílení front byla prováděna kontrola některých zastavení. Ty mohou být přepsány profily, které umožňují kontrolu pro specifické správce front.

Tabulka 30 na stránce 188 zobrazuje profily přepínače používané k řízení přístupu k prostředkům produktu IBM MQ .

Je-li váš správce front součástí skupiny sdílení front a máte-li aktivní zabezpečení skupiny sdílení front a skupiny sdílení front, můžete použít prvek YES.* profil přepínače potlačí profily úrovně skupiny sdílení front a specificky zapne zabezpečení určitého správce front.

Některé profily se vztahují na správce front i skupiny sdílení front. Ty jsou uvedeny předponou řetězce *hlq* a vy byste měli nahradit jméno vaší skupiny sdílení front nebo správce front, jak je vhodné. Názvy profilů s předponou *qmgr-name* jsou přepisující profily správce front. Měli byste nahradit název správce front.

Tabulka 30. Přepnout profily pro kontrolu prostředků

Typ kontroly prostředků, která je řízena	**Název profilu přepínače**	**Přepsat profil pro určitého 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 procesu	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 příkazů	hlq.NO.CMD.RESC.CHECKS	qmgr-name.YES.CMD.RESC.CHECKS
Zabezpečení tématu	hlq.NO.TOPIC.CHECKS	qmgr-name.YES.TOPIC.CHECKS
Poznámka: Generické profily přepínače, jako například hlq.NO. * * jsou ignorovány IBM MQ		

Chcete-li například provést kontroly zabezpečení procesu ve správci front QM01, který je členem skupiny sdílení front QSG3 , ale nechcete provést kontroly zabezpečení procesu u žádného z ostatních správců front ve skupině, definujte následující profily přepínače:

```
QSG3.NO.PROCESS.CHECKS
QM01.YES.PROCESS.CHECKS
```

Chcete-li provést kontroly zabezpečení fronty provedené ve všech správcích front ve skupině sdílení front s výjimkou produktu QM02, definujte následující profil přepínače:

```
QM02.NO.QUEUE.CHECKS
```

(Pro skupinu sdílení front není třeba definovat profil, 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 přepínačů.

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 plnou kontrolu zabezpečení produktu IBM MQ , aby byla aktivní na úrovni skupiny sdílení front v obou systémech.

  To se provádí zadáním následujícího profilu:

  ```
  RDEFINE MQADMIN QS01.NO.QMGR.CHECKS
  ```

  Tato hodnota určuje kontrolu úrovně skupiny sdílení front pro všechny správce front ve skupině sdílení front. Pro provozní správce front nemusíte definovat žádné jiné profily přepínačů, protože chcete zkontrolovat vše pro tyto systémy.
- Při testu správce front MQT1 je vyžadována také úplná kontrola zabezpečení. Vzhledem k tomu, že je však vhodné později změnit, lze zabezpečení definovat na úrovni správce front, abyste mohli změnit nastavení zabezpečení pro tohoto správce front, aniž by to mělo vliv na ostatní členy skupiny sdílení front.

  To provedete tak, že definujete NO.QSG.CHECKS profil pro MQT1 následujícím způsobem:

  ```
  RDEFINE MQADMIN MQT1.NO.QSG.CHECKS
  ```
- Správce front vývoje MQD1 má různé požadavky na zabezpečení ze zbývající skupiny sdílení front. Vyžaduje to pouze připojení a zabezpečení fronty, aby bylo aktivní.

  To lze provést definováním profilu produktu `MQD1.YES.QMGR.CHECKS` pro tohoto správce front a následným definováním následujících profilů pro vypnutí kontroly zabezpečení pro prostředky, které není třeba zkontrolovat:

  ```
  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.

Nastavení přepínače můžete změnit také tehdy, je-li správce front spuštěn definováním nebo odstraněním příslušného profilu přepínače ve třídě MQADMIN. Chcete-li, aby změny nastavení přepínače byly aktivní, je třeba pro třídu MQADMIN zadat příkaz REFRESH SECURITY.

Další informace o použití příkazů DISPLAY SECURITY a REFRESH SECURITY naleznete v příručce “Aktualizace zabezpečení správce front v systému z/OS” na stránce 244 .

z/OS Profily používané k řízení přístupu k prostředkům produktu IBM MQ

Chcete-li řídit přístup k prostředkům produktu IBM MQ , musíte kromě profilů přepínačů, které mohly být definovány, definovat profily produktu RACF . Tato kolekce témat obsahuje informace o profilech produktu RACF pro různé typy prostředků produktu IBM MQ .

Pokud nemáte definován profil prostředku pro konkrétní kontrolu zabezpečení a uživatel vydá požadavek, který by zahrnoval provedení této kontroly, příkaz IBM MQ odepřel přístup. Nemusíte definovat profily pro typy zabezpečení vztahující se k žádným přepínačům zabezpečení, které jste deaktivovali.

z/OS *Profily pro zabezpečení připojení*

Je-li zabezpečení připojení aktivní, je třeba definovat profily ve třídě MQCONN a povolit k těmto profilům přístup nezbytné skupiny nebo ID uživatelů, aby se mohly připojit k produktu IBM MQ.

Chcete-li povolit vytvoření připojení, musíte uživatelům produktu RACF READ udělit přístup k příslušnému profilu. (Pokud neexistuje žádný profil úrovně správce front a váš správce front je členem skupiny sdílení front, mohou být provedeny kontroly nad profily na úrovni skupiny sdílení front, je-li zabezpečení nastaveno tak, aby bylo toto provedeno.)

Profil připojení s názvem správce front řídí přístup ke specifickému správci front a uživatelé s přístupem k tomuto profilu se mohou připojit k danému správci front. Profil připojení kvalifikován názvem skupiny sdílení front řídí přístup ke všem správcům front v rámci skupiny sdílení front pro daný typ připojení. Uživatel s přístupem k produktu `QS01.BATCH` může například používat dávkové připojení k libovolnému správci front ve skupině sdílení front `QS01` , který nemá definován profil úrovně správce front.

Poznámka:

1. Informace o ID uživatelů zkontrolovaných pro různé požadavky na zabezpečení najdete v tématu “ID uživatelů pro kontrolu zabezpečení v systému z/OS” na stránce 233.
2. Kontroly úrovně zabezpečení na úrovni prostředku (RESLEVEL) jsou také prováděny v době připojení. Podrobné informace naleznete v tématu “Profil zabezpečení RESLEVEL” na stránce 227.

Zabezpečení produktu IBM MQ rozpoznává následující různé typy připojení:

- Mezi připojeními typu dávka (a dávkového typu) patří následující:
  - z/OS Dávkové úlohy
  - Aplikace TSO
  - Přihlášení z/OS UNIX System Services
  - Db2Uložené procedury
- CICS připojení
- IMS připojení z řídicích a aplikačních oblastí zpracování
- Inicializátor kanálu IBM MQ

z/OS *Profily zabezpečení připojení pro dávkové připojení*

Profily pro kontrolu spojení typu dávky se skládají ze správce front nebo názvu skupiny sdílení front následovaného slovem *BATCH*. Poskytněte ID uživatele přidružené k připojenému adresnímu prostoru READ přístup k profilu připojení.

Profily pro kontrolu dávkových a dávkových typů připojení mají tento tvar:

```
hlq.BATCH
```

kde `hlq` může být buď `qmgr-name` (název správce front), nebo `qsg-name` (název skupiny sdílení front). Pokud používáte správce front i úroveň skupiny sdílení front, produkt IBM MQ vyhledá předponu s předponou názvu správce front. Pokud ji nenajde, hledá profil s předponou název skupiny sdílení front. Pokud se nepodaří najít žádný profil, požadavek na připojení selže.

Pro dávkové nebo dávkové požadavky na připojení musíte povolit ID uživatele přidruženého k připojenému adresnímu prostoru pro přístup k profilu připojení. Například následující příkaz RACF

umožňuje uživatelům ve skupině CONNTQM1 připojit se ke správci front TQM1; těchto ID uživatelů bude povoleno používat 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 se vztahuje pouze na spojení, která jsou prováděna přes připojení BATCH a nevztahuje se na spojení vyrobená z produktů CICS nebo IMS. Připojení provedená prostřednictvím inicializátoru kanálu jsou řízena produktem **CHCKCLNT**.

Přehled

Chcete-li nakonfigurovat správce front produktu z/OS tak, aby kontroloval ID uživatele a kontrolu hesla pro některé, ale ne všechny lokálně vázané aplikace, je třeba provést další konfiguraci.

Důvodem pro toto je, že jakmile je nakonfigurováno **CHCKLOCL** (*REQUIRED*), starší dávkové aplikace, které používají volání rozhraní API MQCONN, se již nemohou připojovat ke správci front.

Pouze pro systém z/OS lze použít k downgrade globální konfigurace CHCKLOCL (REQUIRED) do CHCKLOCL (VOLITELNÉ) pro specificky definovaná ID uživatele granulární mechanizmus založený na zabezpečení připojení adresního prostoru. Použitý mechanismus je popsán v následujícím textu společně s příkladem.

Chcete-li povolit větší granularitu na **CHCKLOCL** (*REQUIRED*) než pouze EVERYONE, upravíte **CHCKLOCL** stejným způsobem, jak upravíte úroveň přístupu ID uživatele přidruženého k připojenému adresnímu prostoru k profilům připojení `hlq.batch` ve třídě MQCONN.

Pokud má ID uživatele adresního prostoru pouze přístup pro čtení, což je minimum, které vyžadujete k připojení ve všech, použije se konfigurace produktu **CHCKLOCL** jako zapsaná.

Pokud má ID uživatele adresního prostoru přístup UPDATE (nebo vyšší), pak konfigurace **CHCKLOCL** pracuje v *VOLITELNÝ* režimu. To znamená, že nemusíte zadávat ID uživatele a heslo, ale pokud ano, musí být ID uživatele a heslo platnou dvojicí.

Zabezpečení připojení je již konfigurováno pro správce front produktu z/OS

Pokud je pro správce front produktu z/OS konfigurováno zabezpečení připojení a chcete, aby se produkt **CHCKLOCL** (*REQUIRED*) použil pro lokálně vázané aplikace WAS a žádné jiné, proveďte následující kroky:

1. Začni s **CHCKLOCL** (*VOLITELNÝ*) jako svou konfigurací. To znamená, že každé zadané ID uživatele a hesla se kontrolují na platnost, ale nejsou nařízeny.
2. Vypište všechny uživatele, kteří mají přístup k profilům zabezpečení připojení zadáním příkazu:

   ```
   RLIST MQCONN MQ23.BATCH AUTHUSER
   ```

   Tento příkaz se 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 mající přístup pro čtení, změňte přístup na

   ```
   UPDATE:- PERMIT MQ23.BATCH CLASS(MQCONN) ID(JOHNDOE) ACCESS(UPDATE)
   ```

4. Aktualizujte konfiguraci produktu IBM MQ na **CHCKLOCL** (*REQUIRED*).

   Kombinace přístupu UPDATE k produktu `MQ23.BATCH` a aktuálního nastavení znamená, že používáte produkt **CHCKLOCL** (*VOLITELNÝ*).
5. Nyní použijte chování **CHCKLOCL** (*REQUIRED*) na jedno specifické ID uživatele, například `WASUSER`, takže všechna připojení přicházející z této oblasti musí poskytovat ID uživatele a heslo.

   Proveďte to tím, že změníte dříve provedené změny zadáním následujícího příkazu:

```
PERMIT MQ23.BATCH CLASS(MQCONN) ID(WASUSER) ACCESS(READ)
```

Zabezpečení připojení není konfigurováno pro správce front produktu z/OS

V této situaci musíte:

1. Vytvořte profily připojení pro produkt `hlq.BATCH` ve třídě MQCONN zadáním následujícího příkazu:

```
RDEFINE MQCONN MQ23.BATCH UACC(NONE)
```

2. Autorizujte všechna ID uživatelů, která vytvářejí dávková připojení ke správci front, aby měli k tomuto profilu přístup UPDATE. Tím dojde k vynechání požadavku **CHCKLOCL** (*REQUIRED*) pro ID uživatele a heslo v době připojení.

   Proveďte to zadáním následujícího příkazu:

```
PERMIT MQ23.BATCH CLASS(MQCONN)ID(JOHNDOE) ACCESS(UPDATE)
```

   Ty zahrnují ID uživatelů:

   a. Používá se pro panely CSQUTIL, ISPF a další lokálně vázané nástroje.
   b. Přidruženo k dávkovému zpracování jako připojení ke správci front. Zvažte například například Advanced Message Security, IBM Integration Bus, uložené procedury Db2 , uživatele z/OS UNIX System Services a TSO a aplikace Java .
3. Zadáním následujícího příkazu odstraňte profil přepínače pro správce front:

```
hlq.NO.CONNECT.CHECKS
```

4. Nyní použijte chování **CHCKLOCL** (*REQUIRED*) na jedno specifické ID uživatele, například `WASUSER`, takže všechna připojení přicházející z této oblasti musí poskytovat ID uživatele a heslo.

   Proveďte to tím, že změníte dříve provedené změny zadáním následujícího 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 názvu skupiny sdílení front následovaného slovem *CICS* . Poskytněte ID uživatele přidružené k adresnímu prostoru CICS READ přístup k profilu připojení.

Profily pro kontrolu připojení z produktu CICS mají tento tvar:

```
hlq.CICS
```

kde `hlq` může být buď `qmgr-name` (název správce front), nebo `qsg-name` (název skupiny sdílení front). Pokud používáte správce front i úroveň skupiny sdílení front, produkt IBM MQ vyhledá předponu

s předponou názvu správce front. Pokud ji nenajde, hledá profil s předponou název skupiny sdílení front. Pokud se nepodaří najít žádný profil, požadavek na připojení selže.

Pro požadavky na připojení od CICSmusíte povolit pouze přístup ID uživatele adresního prostoru CICS k profilu připojení.

Například následující příkazy RACF umožňují uživateli adresního prostoru CICS adresovat ID uživatele KCBCICS pro připojení 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 názvu skupiny sdílení front následovaného slovem *IMS* . Zadejte ID uživatele pro řízení IMS a ID uživatelů závislých oblastí READ pro přístup k profilu připojení.

Profily pro kontrolu připojení z produktu IMS mají tento tvar:

```
hlq.IMS
```

kde `hlq` může být buď `qmgr-name` (název správce front), nebo `qsg-name` (název skupiny sdílení front). Pokud používáte správce front i úroveň skupiny sdílení front, produkt IBM MQ vyhledá předponu s předponou názvu správce front. Pokud ji nenajde, hledá profil s předponou název skupiny sdílení front. Pokud se nepodaří najít žádný profil, požadavek na připojení selže.

Pro požadavky na připojení pomocí IMSpovolte přístup k profilu připojení pro řídicí a uživatelská ID závislých oblastí produktu IMS .

Například následující příkazy RACF umožňují:

- ID uživatele oblasti IMS , IMSREG, pro připojení ke správci front TQM1.
- Uživatelé ve skupině BMPGRP k 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 ze správce front nebo názvu skupiny sdílení front následovaného slovem *CHIN*. Zadejte ID uživatele použité inicializatorem kanálu s přístupem k profilu připojení READ k profilu připojení.

Profily pro kontrolu připojení od inicializátoru kanálu mají následující tvar:

```
hlq.CHIN
```

kde `hlq` může být buď `qmgr-name` (název správce front), nebo `qsg-name` (název skupiny sdílení front). Pokud používáte správce front i úroveň skupiny sdílení front, produkt IBM MQ vyhledá předponu s předponou názvu správce front. Pokud ji nenajde, hledá profil s předponou název skupiny sdílení front. Pokud se nepodaří najít žádný profil, požadavek na připojení selže.

Pro požadavky na připojení pomocí inicializátoru kanálu definujte přístup k profilu připojení pro ID uživatele použité adresním prostorem úlohy iniciátoru kanálu.

Například následující příkazy produktu RACF umožňují připojení adresního prostoru inicializátoru kanálu s ID uživatele DQCTRL k připojení 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, je třeba definovat profily v příslušných třídách a povolit k těmto profilům přístup nezbytné skupiny nebo ID uživatelů. Profily zabezpečení fronty jsou pojmenovány podle správce front nebo skupiny sdílení front a fronty, která má být otevřena.

Je-li zabezpečení fronty aktivní, musíte:

- Definujte profily ve třídách **MQQUEUE** nebo **GMQQUEUE** , pokud používáte velké profily.
- Definujte profily ve třídách **MXQUEUE** nebo **GMXQUEUE** v případě použití smíšených profilů případu.
- Povolte nezbytné skupiny nebo ID uživatelů pro přístup k těmto profilům, aby mohli vydat požadavky rozhraní API produktu IBM MQ , které používají fronty.

Profily pro zabezpečení fronty mají formu:

```
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 v 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 daným názvem fronty ve všech správcích front v rámci skupiny sdílení front, nebo přístup ke sdílené frontě libovolného správce front v rámci skupiny. Tento přístup lze potlačit pro jednotlivé správce front definováním profilu úrovně správce front pro danou frontu v daném správci front.

Je-li váš správce front členem skupiny sdílení front a používáte-li správce front i zabezpečení na úrovni skupiny sdílení front, produkt IBM MQ nejprve zkontroluje profil s předponou názvu správce front. Pokud ji nenajde, hledá profil s předponou název skupiny sdílení front.

Používáte-li sdílené fronty, doporučuje se používat zabezpečení na úrovni skupiny sdílení front.

Podrobnosti o tom, jak zabezpečení fronty pracuje, je-li název fronty alias alias nebo fronty modelu z/OS, viz “Pokyny pro alias fronty” na stránce 196 a “Pokyny pro modelové fronty” na stránce 197 .

Přístup produktu RACF vyžadovaný k otevření fronty závisí na zadaných volbách `MQOPEN` nebo `MQPUT1` . Je-li více než jedna z voleb MQOO_ * a MQPMO_ * kódována, je kontrola zabezpečení fronty provedena pro nejvyšší požadované oprávnění RACF .

Tabulka 31. Úrovně přístupu pro zabezpečení fronty pomocí volání MQOPEN nebo MQPUT1

Volba MQOPEN nebo MQPUT1	**Úroveň přístupu produktu RACF je vyžadována pro hlq.queuename .**
MQOOK_BROWSE	READ (čtení)
MQO_ DOTÁZAT SE	READ (čtení)
MQOO_BIND_*	AKTUALIZOVAT

Tabulka 31. Úrovně přístupu pro zabezpečení fronty pomocí volání MQOPEN nebo MQPUT1 (pokračování)	
Volba MQOPEN nebo MQPUT1	**Úroveň přístupu produktu RACF je vyžadována pro hlq.queuename .**
MQO_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
ÁLNÍ_KONTEXT MQOO_SAVE_ALL_CONTEXT	AKTUALIZOVAT
MQOO_SET_IDENTITY_CONTEXT MQPMO_SET_IDENTITY_CONTEXT	AKTUALIZOVAT
MQO_SET_ALL_CONTEXT MQPMO_SET_ALL_CONTEXT	AKTUALIZOVAT
MQOOK_SADA	ALTER

Například u správce front IBM MQ QM77mají být všechna ID uživatelů ve skupině RACF PAYGRP udělen přístup k získání zpráv z nebo vkládání zpráv do všech front s názvy začínajícími na 'PAY.'. To lze provést pomocí těchto příkazů obslužného programu 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 nepostupují podle konvence 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 zpřístupováním této třídy 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. Pokud se změní úroveň přístupu produktu RACF , kterou má aplikace do profilu zabezpečení fronty, projeví se změny pouze pro všechny nové získané popisovače objektů (tj. pro novou frontu MQOPEN) pro danou frontu. Tyto popisovače již existující v době změny si uchovají svůj stávající přístup do fronty. Je-li požadována aplikace pro použití změněné úrovně přístupu k frontě spíše než na existující úrovni 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.

Další typy kontrol zabezpečení se mohou také vyskytnout v době otevření fronty v závislosti na zadaných volbách otevření a typech zabezpečení, které jsou aktivní. z/OS Viz také “Profily pro zabezpečení kontextu” na stránce 211 a “Profily pro alternativní zabezpečení uživatelů” na stránce 209. U souhrnné tabulky zobrazující volby otevření a autorizace zabezpečení potřebné pro zařazení do fronty, kontext a alternativní zabezpečení uživatele jsou všechny aktivní, viz Tabulka 36 na stránce 202.

Pokud používáte publikování/odběr, je třeba vzít v úvahu následující informace: Při zpracování požadavku MQSUB je provedena kontrola zabezpečení, aby bylo zajištěno, že ID uživatele, který požadavek provádí, má požadovaný přístup k vkládání zpráv do cílové fronty IBM MQ a také požadovaný přístup k odběru tématu produktu IBM MQ .

Tabulka 32. Úrovně přístupu pro zabezpečení fronty pomocí volání MQSUB

Volba MQSUB	**Úroveň přístupu produktu RACF je vyžadována pro hlq.queuename .**
MQSO_ALTER, MQSO_CREATE, a MQSO_RESUME	AKTUALIZOVAT

Poznámka:

1. `hlq.queuename` je cílová fronta pro publikování. Pokud se jedná o spravovanou frontu, potřebujete přístup k příslušné modelové frontě, která má být použita pro spravovanou frontu a pro dynamickou frontu, která je vytvořena.
2. Tuto techniku můžete použít pro cílovou frontu, kterou jste zadali ve volání rozhraní MQSUB API, chcete-li rozlišovat mezi uživateli, kteří provádějí odběry, a uživatelům, kteří načítají publikování z cílové fronty.

z/OS *Pokyny pro alias fronty*

Když zadáte volání `MQOPEN` nebo `MQPUT1` pro frontu aliasů, produkt IBM MQ provede kontrolu prostředku proti názvu fronty uvedenému v deskriptoru objektu (MQOD) na volání. Nekontroluje, zda má uživatel povolen přístup k názvu cílové fronty.

Příklad: alias fronta s názvem PAYROLL.REQUEST se interpretuje jako cílová fronta PAY.REQUEST. Je-li zabezpečení fronty aktivní, musíte mít oprávnění pouze pro přístup ke frontě PAYROLL.REQUEST. Neprovede se žádná kontrola, abyste zjistili, zda máte oprávnění pro přístup do fronty 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 *Pokyny pro modelové fronty*

Chcete-li otevřít modelovou frontu, musíte mít možnost otevřít jak samotnou modelovou frontu, tak i dynamickou frontu, na kterou se řeší. Definujte generické profily produktu RACF pro dynamické fronty, včetně dynamických front používaných obslužnými programy produktu IBM MQ .

Když otevřete modelovou frontu, zabezpečení produktu IBM MQ provede dvě kontroly zabezpečení fronty:

1. Jste autorizováni pro přístup k modelové frontě?
2. Jste autorizováni pro přístup k dynamické frontě, na kterou je modelová fronta vyřešena?

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 vygenerovaného řetězce, měli byste definovat generické profily pro tyto fronty.

Volání MQOPEN například používá název modelové fronty CREDIT.CHECK.REPLY.MODEL a název dynamické fronty CREDIT.REPLY.* ve správci front (nebo ve skupině sdílení front) MQSP.

Chcete-li to provést, je třeba při definování nezbytných profilů fronty zadat následující příkazy produktu RACF :

```
RDEFINE MQQUEUE MQSP.CREDIT.CHECK.REPLY.MODEL
RDEFINE MQQUEUE MQSP.CREDIT.REPLY.**
```

Chcete-li umožnit uživateli přístup k těmto profilům, musíte také zadat odpovídající příkazy RACF PERMIT.

Typický název dynamické fronty vytvořený operací MQOPEN je něco jako CREDIT.REPLY.A346EF00367849A0. Přesná hodnota posledního kvalifikátoru je nepředvídatelná; proto byste měli používat generické profily pro tyto názvy front.

Počet zpráv obslužných programů produktu IBM MQ vkládaného do dynamických front. Profily byste měli definovat pro následující dynamické názvy front a poskytnout přístup pro příkaz RACF UPDATE k příslušným ID uživatelů (viz “ID uživatelů pro kontrolu zabezpečení v systému z/OS” na stránce 233 , kde jsou uvedena správná ID uživatelů):

```
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 dynamického názvu fronty použitého při výchozím nastavení v členech programu pro kopírování aplikací. Kopípisové knihy dodané IBM MQobsahují výchozí *DynamicQName*, což je CSQ. *. Tím je umožněno vytvoření odpovídajícího profilu RACF .

Poznámka: Nepovolujte programátorům aplikací zadat pro název dynamické fronty hodnotu jedinou *. Pokud ano, musíte definovat hlq. * * profilu ve třídě MQQUEUE a vy jej budete muset poskytnout v rámci přístupu k přístupu. To znamená, že tento profil může být použit i pro jiné nedynamické fronty, které nemají specifičtější profil RACF . Vaši uživatelé tak mohou získat přístup k frontám, do kterých nechcete, aby měli přístup.

z/OS *Volby zavření u trvalých dynamických front*

Pokud aplikace otevře trvalou dynamickou frontu, která byla vytvořena jinou aplikací, a poté se pokusí tuto frontu odstranit pomocí volby MQCLOSE , budou při pokusu o provedení pokusu provedeny některé další kontroly zabezpečení.

Tabulka 33. Úrovně přístupu pro trvalé volby v trvalých dynamických frontách

volba MQCLOSE	**Úroveň přístupu produktu RACF je vyžadována pro hlq.queuename .**
MQCO_DELETE	ALTER
MQCO_DELETE_PURGE	ALTER

z/OS *Zabezpečení a vzdálené fronty*

Když je zpráva vložena do vzdálené fronty, závisí zabezpečení fronty, které je implementováno lokálním správcem front, na tom, jak je vzdálená fronta zadána při jeho otevření.

Jsou použita následující pravidla:

1. Pokud byla vzdálená fronta definována v lokálním správci front prostřednictvím příkazu IBM MQ DEFINE QREMOTE, je zaškrtnutá fronta názvem vzdálené fronty. Je-li 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 definován ve třídě MQQUEUE.

2. Pokud se položka *ObjectQMgr* pro daný požadavek neinterpretuje jako lokální správce front, provede se kontrola zabezpečení proti vyřešenému (vzdálenému) správci front s výjimkou případu fronty klastru, kde je provedena kontrola nad názvem fronty klastru.

   Například přenosová fronta BANK1.TO.BANK7 je definován ve správci front MQS1. Požadavek MQPUT1 je poté zadán v systému MQS1 zadáním řetězce *ObjectName* jako BANK1.INTERBANK.TRANSFERS a *ObjectQMgrName* z BANK1.TO.BANK7. V takovém případě musí mít uživatel provádějící požadavek přístup k BANK1.TO.BANK7.

3. Provedete-li požadavek MQPUT do fronty a jako název aliasu lokálního správce front zadáte *ObjectQMgrName* , bude zkontrolováno pouze název fronty zabezpečení, nikoli správce front.

Když se zpráva dostane do vzdáleného správce front, může být předmětem dalšího zabezpečení zpracování. Další informace viz téma “Zabezpečení pro vzdálený systém zpráv” na stránce 94.

z/OS *Zabezpečení fronty nedoručených zpráv*

Speciální pokyny platí pro frontu nedoručených zpráv, protože mnoho uživatelů musí mít možnost vkládat zprávy do fronty, ale přístup k načítaným zprávám musí být přísně omezen. Toho lze dosáhnout použitím různých oprávnění správce RACF k frontě nedoručených zpráv a alias fronty.

Nedoručené zprávy lze vložit do speciální fronty s názvem fronty nedoručených zpráv. Pokud máte citlivá data, která by mohla skončit v této frontě, musíte vzít v úvahu její důsledky, protože nechcete, aby uživatelé tyto údaje načetli neautorizovaní uživatelé.

Každá z následujících položek musí mít povoleno vkládat zprávy do fronty nedoručených zpráv:

- Aplikační programy.
- Adresní prostor inicializátoru kanálu a všechna ID uživatele MCA. (Pokud profil RESLEVEL není přítomen nebo je definován tak, že ID uživatele kanálu jsou zaškrtnuty, ID uživatele kanálu také potřebuje oprávnění k umístění zpráv do fronty nedoručených zpráv.)
- CKTI, the CICS-supplied CICS task initiator.
- CSQQTRMN, the IBM MQ-supplied IMS trigger monitor.

Jediná aplikace, která může načítat zprávy z fronty nedoručených zpráv, by měla být 'speciální' aplikace, která zpracovává tyto zprávy. Problém však vzniká v případě, že poskytnete aplikacím RACF UPDATE oprávnění pro frontu 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 ano, ani ty 'speciální' aplikace nemohou načíst zprávy.

Jedním řešením tohoto problému je nastavit dvouúrovňový přístup k frontě zablokovaných dopisů. CKTI, transakce agenta kanálu zpráv nebo adresní prostor iniciátoru kanálu a 'speciální' aplikace mají přímý přístup; ostatní aplikace mohou přistupovat k frontě zablokovaných zpráv pouze prostřednictvím alias fronty. Tento alias je definován tak, aby povoloval aplikacím vkládat zprávy do fronty nedoručených zpráv, ale neodesílat zprávy z něj.

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 pro následující ID uživatelů:
   - ID uživatele, pod kterými běží CKTI a MCAs nebo adresní prostor iniciátoru kanálu.
   - ID uživatelů přidružená ke zpracování 'speciální' fronty zpracování nedoručených zpráv.
3. Definujte frontu aliasů, která bude převedena na skutečnou frontu nedoručených zpráv, ale dejte alias frontu těchto atributů: PUT (ENABLED) a GET (DISABLED). Zadejte alias fronty název se stejným kmenem jako název fronty nedoručených zpráv, ale připojte znaky ". PUT" k tomuto kmeni. Je-li například název fronty s dead-letter hlq.DEAD.QUEUE, alias fronty aliasů by byl hlq.DEAD.QUEUE.PUT.
4. Chcete-li vložit zprávu do fronty nedoručených zpráv, aplikace použije alias frontu. To musí vaše aplikace dělat:
   - Načtěte název skutečné fronty nedoručených zpráv. Chcete-li tak učinit, otevře objekt správce front pomocí příkazu MQOPEN a poté vydá příkaz MQINQ , aby získal název fronty nedoručených zpráv.
   - Sestavte název fronty aliasů přidáním znaků '.PUT' do tohoto názvu, v tomto případě, hlq.DEAD.QUEUE.PUT.
   - Otevřete alias frontu hlq.DEAD.QUEUE.PUT.
   - Vložte zprávu do fronty skutečných nedoručených zpráv zadáním příkazu MQPUT pro alias frontu.
5. Poskytněte ID uživatele přidružené k aplikaci RACF UPDATE oprávnění k aliasu, ale nemá přístup (oprávnění NONE) k skutečné frontě nedoručených zpráv. To znamená, že:
   - Aplikace může vkládat zprávy do fronty nedoručených zpráv pomocí fronty aliasů.
   - Aplikace nemůže načíst zprávy z fronty nedoručených zpráv s použitím fronty aliasů, protože fronta aliasů je zakázaná pro operace get.

Aplikace nemůže získat žádné zprávy ze skutečné fronty nedoručených zpráv, protože má správné oprávnění RACF .

Tabulka 34 na stránce 200 shrnuje oprávnění RACF požadované pro různé účastníky tohoto řešení.

Tabulka 34. Oprávnění správce RACF k frontě nedoručených zpráv a její alias

ID přidružených uživatelů	**Skutečná fronta nedoručených zpráv (hlq.DEAD.QUEUE)**	**Alias fronta nedoručených zpráv (hlq.DEAD.QUEUE.PUT)**
Název adresního prostoru MCA nebo inicializátor kanálu a CKTI	AKTUALIZOVAT	ŽÁDNÉ
'Speciální' aplikace (pro zpracování fronty nedoručených zpráv)	AKTUALIZOVAT	ŽÁDNÉ
ID uživatele aplikace zapsaná uživatelem	ŽÁDNÉ	AKTUALIZOVAT

Použijete-li tuto metodu, aplikace nemůže určit maximální délku zprávy (MAXMSGL) ve frontě nedoručených zpráv. Důvodem je skutečnost, že atribut MAXMSGL nelze načíst z alias fronty. Proto by vaše aplikace měla předpokládat, že maximální délka zprávy je 100 MB, maximální velikost IBM MQ for z/OS podporuje. Skutečná fronta nedoručených zpráv by měla být také definována s atributem MAXMSGL o velikosti 100 MB.

Poznámka: Uživatelem napsané aplikační programy obvykle nepoužívají alternativní oprávnění uživatele k umístění zpráv do fronty nedoručených zpráv. Tím se sníží počet ID uživatelů, kteří mají přístup k frontě nedoručených zpráv.

z/OS *Zabezpečení systémové fronty*

Chcete-li povolit určitým systémovým frontám přístup ke konkrétním systémovým frontám, je třeba nastavit přístup produktu RACF .

Pomocným částem IBM MQpřistupuje k mnoha frontám systému:

- Obslužný program CSQUTIL
- Obslužný program zásad zabezpečení zpráv (CSQ0UTIL)
- Ovládací panely a ovládací panely
- Adresní prostor inicializátoru kanálu (včetně démona publikování/odběru ve frontě)
- Server mqweb používaný produkty MQ Console a REST API.

ID uživatelů, pod kterým tyto spuštění musí být udělen RACF přístup k těmto frontám, jak je zobrazeno v Tabulka 35 na stránce 200.

Tabulka 35. Přístup požadovaný pro fronty SYSTEM pomocí IBM MQ

Fronta SYSTEM	**KALKUNIT**	**CSQ0UTIL**	**mqweb server**	**Ovládací panely a ovládací panely**	**Inicializátor kanálu pro distribuované fronty**
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

Tabulka 35. Přístup požadovaný pro fronty SYSTEM pomocí IBM MQ (pokračování)

Fronta SYSTEM	KALKUNIT	CSQ0UTIL	mqweb server	Ovládací panely a ovládací panely	Inicializátor kanálu pro distribuované fronty
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
SYSTEM.PROTECTION.ERROR.QUEUE	-	-	-	-	AKTUALIZOVAT
SYSTEM.PROTECTION.POLICY.QUEUE	-	Aktualizovat“1” na stránce 202	-	-	READ (čtení)
SYSTEM.QSG.CHANNEL.SYNCQ	-	-	-	-	AKTUALIZOVAT
SYSTEM.QSG.TRANSMIT.QUEUE	-	-	-	-	AKTUALIZOVAT

Tabulka 35. Přístup požadovaný pro fronty SYSTEM pomocí IBM MQ (pokračování)					
Fronta SYSTEM	**KALKUNIT**	**CSQ0UTIL**	**mqweb server**	**Ovládací panely a ovládací panely**	**Inicializátor kanálu pro distribuované fronty**
SYSTEM.REST.REPLY.QUEUE	-	-	AKTUALIZOVAT	-	-
SYSTEM.BLUEMIX.REGISTRATION.QUEUE	-	-	-	-	AKTUALIZOVAT

Notes:

1. Uživatel adresního prostoru produktu Advanced Message Security také vyžaduje přístup READ k této frontě.

z/OS *Rozhraní API-rychlý odkaz na zabezpečení přístupu k prostředkům*

Souhrn voleb **MQOPEN**, **MQPUT1**, **MQSUB**a **MQCLOSE** a přístup požadovaný různými typy zabezpečení prostředků.

Tabulka 36. Volby MQOPEN, MQPUT1, MQSUB a MQCLOSE a požadovaná autorizace zabezpečení. Bubliny zobrazené jako tento **(1)** odkazují na poznámky následující za touto tabulkou.				
	Požadovaná minimální 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				
MQO_ DOTÁZAT SE		READ **(5)**	Žádná kontrola	Žádná kontrola
MQOOK_BROWSE		READ (čtení)	Žádná kontrola	Žádná kontrola
MQO_INPUT_*		AKTUALIZOVAT	Žádná kontrola	Žádná kontrola
MQOO_SAVE_ALL_CONTEXT **(6)**		AKTUALIZOVAT	Žádná kontrola	Žádná kontrola
MQOO_OUTPUT (USAGE = NORMAL) **(7)**		AKTUALIZOVAT	Žádná kontrola	Žádná kontrola
MQOO_PASS_IDENTITY_CONTEXT **(8)**		AKTUALIZOVAT	READ (čtení)	Žádná kontrola
MQOO_PASS_ALL_CONTEXT **(8) (9)**		AKTUALIZOVAT	READ (čtení)	Žádná kontrola
MQOO_SET_IDENTITY_CONTEXT **(8) (9)**		AKTUALIZOVAT	AKTUALIZOVAT	Žádná kontrola
MQOO_SET_ALL_CONTEXT **(8) (10)**		AKTUALIZOVAT	CONTROL	Žádná kontrola

Tabulka 36. Volby MQOPEN, MQPUT1, MQSUB a MQCLOSE a požadovaná autorizace zabezpečení. Bubliny zobrazené jako tento **(1)** odkazují na poznámky následující za touto tabulkou. *(pokračování)*

	Požadovaná minimální 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_OUTPUT (USAGE (XMITQ) **(11)**		AKTUALIZOVAT	CONTROL	Žádná kontrola
MQOO_OUTPUT (objekt tématu)	UPDATE **(16)**			
MQOO_OUTPUT (alias fronty k objektu tématu)	UPDATE **(16)**	AKTUALIZOVAT		
MQOOK_SADA		ALTER	Žádná kontrola	Žádná kontrola
MQO_ALTERNATE_USER_AUTHORITY.		**(12)**	**(12)**	AKTUALIZOVAT
Volba MQPUT1				
Vložení do normální fronty **(7)**		AKTUALIZOVAT	Žádná kontrola	Žádná kontrola
KONTEXT MQPMO_PASS_IDENTITY_CONTEXT		AKTUALIZOVAT	READ (čtení)	Žádná kontrola
MQPMO_PASS_ALL_CONTEXT		AKTUALIZOVAT	READ (čtení)	Žádná kontrola
KONTEXT MQPMO_SET_IDENTITY_CONTEXT		AKTUALIZOVAT	AKTUALIZOVAT	Žádná kontrola
MQPMO_SET_ALL_CONTEXT		AKTUALIZOVAT	CONTROL	Žádná kontrola
MQOOK_VÝSTUP Vložení do přenosové fronty **(11)**		AKTUALIZOVAT	CONTROL	Žádná kontrola
MQOO_OUTPUT (objekt tématu)	UPDATE **(16)**			
MQOO_OUTPUT (alias fronty k objektu tématu)	UPDATE **(16)**	AKTUALIZOVAT		
MQPMO_ALTERNATE_USER_AUTHORITY		**(13)**	**(13)**	AKTUALIZOVAT
Volba MQCLOSE				
MQCO_DELETE **(14)**		ALTER	Žádná kontrola	Žádná kontrola
MQCO_DELETE_PURGE **(14)**		ALTER	Žádná kontrola	Žádná kontrola
MQCO_REMOVE_SUB	ALTER **(15)**			
Volba MQSUB				

Tabulka 36. Volby MQOPEN, MQPUT1, MQSUB a MQCLOSE a požadovaná autorizace zabezpečení. Bubliny zobrazené jako tento **(1)** odkazují na poznámky následující za touto tabulkou. *(pokračování)*

	Požadovaná minimální úroveň přístupu RACF			
RACF Třída:	**MXTOPIC**	**MQQUEUE nebo MXQUEUE (1)**	**MQADMIN nebo MXADMIN**	**MQADMIN nebo MXADMIN**
RACF Profil:	**(15 nebo 16)**	**(2)**	**(3)**	**(4)**
VYTVOŘENÉ MQSO_CREATE	ALTER **(15)**	**(17)**	**(18)**	
MQSO_ALTER	ALTER **(15)**	**(17)**	**(18)**	
MQSO_RESUME	READ **(15)**	**(17)**	Žádná kontrola	
OPRÁVNĚNÍ UŽIVATELE MQSO_ALTERNATE_USER_AUTHORITY				AKTUALIZOVAT
KONTEXT MQSO_SET_IDENTITY_CONTEXT			**(18)**	

Poznámka:

1. Tato volba není omezena na fronty. Použijte třídu MQNLIST nebo MXNLIST pro seznamy názvů a třídu MQPROC nebo MXPROC pro procesy.
2. Použít profil produktu RACF : hlq.resourcename
3. Použijte profil produktu RACF : hlq.CONTEXT.queuename
4. Použijte profil produktu RACF : hlq.ALTERNATE.USER. `alternateuserid`

   `alternateuserid` je identifikátor uživatele, který je zadán v poli *`AlternateUserId`* v deskriptoru objektu. Všimněte si, že pro tuto kontrolu se použije až 12 znaků z pole *`AlternateUserId`* , na rozdíl od jiných kontrol, kde se používají pouze prvních 8 znaků identifikátoru uživatele.
5. Při otevírání správce front pro dotazy se nekontroluje žádná kontrola.
6. Musí být zadán také parametr 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). Je-li fronta vzdálenou frontou, která je otevřena zadáním *`ObjectQMgrName`* (nikoli názvu připojeného správce front) explicitně, provede se kontrola ve frontě se stejným názvem jako *`ObjectQMgrName`* (což musí být lokální fronta s atributem fronty **Usage** MQUS_TRANSMISION).
8. Musí být zadán také MQOO_OUTPUT.
9. Tuto volbu má také implikovaná hodnota MQO_P_PASS_IDENTITY_CONTEXT.
10. Tato volba zahrnuje i MQOO_PASS_IDENTITY_CONTEXT, MQOO_PASS_ALL_CONTEXT a MQOO_SET_IDENTITY_CONTEXT.
11. Tato kontrola se provádí pro lokální nebo modelovou frontu, která má atribut fronty **Usage** MQUS_TRANSMISSION, a je otevírány přímo pro výstup. Nepoužije se, je-li otevřena vzdálená fronta.
12. Musí být zadán alespoň jeden z příkazů MQOO_INQUIRE, MQOO_BROWSE, MQOO_INPUT_ *, MQOO_OUTPUT nebo MQOO_SET. Kontrola prováděná je stejná jako u ostatních zadaných voleb.
13. Kontrola prováděná je stejná jako u ostatních zadaných voleb.
14. Toto platí pouze pro trvalé dynamické fronty, které byly otevřeny přímo, tj. neotevřené přes modelovou frontu. K odstranění dočasné dynamické fronty není vyžadováno žádné zabezpečení.
15. Použijte profil produktu RACF hlq.SUBSCRIBE.topicname.
16. Použijte profil produktu RACF hlq.PUBLISH.topicname.

17. Pokud jste v požadavku MQSUB zadali cílovou frontu pro publikování, která má být odeslána, provede se kontrola zabezpečení proti této frontě, abyste se ujistili, že jste do této fronty zadali oprávnění.
18. Pokud v požadavku MQSUB s uvedenými volbami MQSO_CREATE nebo MQSO_ALTER chcete nastavit libovolné pole kontextu identity ve struktuře MQSD, je nutné zadat také volbu MQSO_SET_IDENTITY_CONTEXT a také pro cílovou frontu potřebujete příslušné oprávnění k profilu kontextu.

z/OS *Profily pro zabezpečení témat*

Je-li zabezpečení tématu aktivní, je třeba definovat profily v příslušných třídách a povolit k těmto profilům přístup nezbytné skupiny nebo uživatelská jména.

Koncepce zabezpečení tématu v rámci stromu témat je popsána v tématu Zabezpečení publikování/odběru.

Je-li zabezpečení tématu aktivní, je třeba provést následující akce:

- Definujte profily ve třídách **MXTOPIC** nebo **GMXTOPIC** .
- Povolte k těmto profilům přístup nezbytné skupiny nebo ID uživatelů, aby mohli vydat požadavky rozhraní API produktu IBM MQ , které používají témata.

Profily pro zabezpečení témat mají tento tvar:

```
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 přidružený buď k odběru tématu prostřednictvím volání MQSUB nebo je publikován prostřednictvím volání MQOPEN.

Profil s předponou v názvu správce front řídí přístup k jedinému 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 potlačit pro jednotlivé správce front definováním profilu úrovně správce front pro dané téma v daném správci front.

Je-li váš správce front členem skupiny sdílení front a používáte-li správce front i zabezpečení na úrovni skupiny sdílení front, produkt IBM MQ nejprve zkontroluje profil s předponou názvu správce front. Pokud ji nenajde, hledá profil s předponou název skupiny sdílení front.

Odebírat

Chcete-li se přihlásit k odběru tématu, musíte mít přístup k tématu, k jehož odběru se chcete přihlásit, a k cílové frontě pro publikování.

Když zadáte požadavek MQSUB, dojde k následujícím kontrolám zabezpečení:

- Zda máte k dispozici příslušnou úroveň přístupu k odběru daného tématu, a také že cílová fronta (je-li zadána) je otevřena pro výstup
- Zda máte odpovídající úroveň přístupu k této cílové frontě.

Tabulka 37. Úroveň přístupu vyžadovaná pro zabezpečení tématu k odběru

Volba MQSUB	**RACF access required to `hlq.SUBSCRIBE.topicname` profile in MXTOPIC class**
MQSO_CREATE a MQSO_ALTER	ALTER
MQSO_RESUME	READ (čtení)

Tabulka 38. Další oprávnění vyžadované pro přihlášení k odběru pomocí nespravované cílové fronty	
Volba MQSUB	**V třídě MQADMIN nebo MXADMIN je požadován přístup produktu RACF k profilu produktu `hlq.CONTEXT.queuename`**
MQSO_CREATE, MQSO_ALTER, a MQSO_RESUME	AKTUALIZOVAT
	RACF přístup nezbytný k profilu `hlq.queuename` ve třídě MQQUEUE nebo MXQUEUE
MQSO_CREATE a MQSO_ALTER	AKTUALIZOVAT
	RACF přístup požadovaný k profilu `hlq.ALTERNATE.USER.alternateuserid` ve třídě MQADMIN nebo MXADMIN
OPRÁVNĚNÍ UŽIVATELE MQSO_ALTERNATE_USER_AUTHORITY	AKTUALIZOVAT

Pokyny pro spravované fronty pro odběry

Je provedena kontrola zabezpečení, abyste zjistili, zda máte oprávnění přihlásit se k odběru tématu. Při vytvoření spravované fronty se však neprovádějí žádné kontroly zabezpečení nebo pokud chcete určit, zda máte přístup k vkládání zpráv 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.

Neposkytujte žádné uživateli přístup k těmto frontám. Fronty mohou být chráněny pomocí generických profilů ve tvaru `SYSTEM.MANAGED.DURABLE.*` a `SYSTEM.MANAGED.NDURABLE.*` bez udělených oprávnění.

Zprávy lze z těchto front načíst pomocí manipulátoru vráceného v požadavku MQSUB.

Pokud jste explicitně zadali volání MQCLOSE pro odběr s určenou volbou MQCO_REMOVE_SUB a nevytvořili jste odběr, který jste uzavřeli pod tímto popisovačem, provede se kontrola zabezpečení v době uzavření, abyste se ujistili, že máte správné oprávnění k provedení této operace.

Tabulka 39. Úroveň přístupu vyžadovaná pro profily zabezpečení tématu pro uzavření operace odběru	
volba MQCLOSE	**RACF access required to `hlq.SUBSCRIBE.topicname` profile in MXTOPIC class**
MQCO_REMOVE_SUB	ALTER

Publikovat

Chcete-li publikovat na téma, které potřebujete k tématu, a pokud používáte alias fronty, také do fronty alias.

Tabulka 40. Úroveň přístupu vyžadovaná pro zabezpečení tématu pro publikování	
Volba MQOPEN nebo MQPUT1	**RACF access required to `hlq.PUBLISH.topicname` profile in MXTOPIC class**
MQOO_OUTPUT nebo MQPUT1	AKTUALIZOVAT

Tabulka 41. Úroveň přístupu vyžadovaná pro otevření fronty aliasů, která se vyřeší na téma	
Volba MQOPEN nebo MQPUT1	**RACF přístup k profilu produktu `hlq.queuename` ve třídě MQQUEUE nebo MXQUEUE pro frontu aliasů**
MQOO_OUTPUT nebo MQPUT1	AKTUALIZOVAT

Podrobnosti o tom, jak zabezpečení tématu funguje, když je otevřena fronta aliasů, která se řeší jako název tématu, je otevřena pro publikování, viz “Aspekty pro fronty aliasů, které se interpretují na témata pro operaci publikování” na stránce 207.

Při použití alias front aliasů použitých pro cílové fronty pro omezení PUT nebo GET viz “Pokyny pro alias fronty” na stránce 196.

Změní-li se úroveň přístupu produktu RACF na profil zabezpečení tématu, projeví se změny pouze u všech získaných nových manipulátorů objektů (tj. pro nové MQSUB nebo MQOPEN) daného tématu. Tyto popisovače již existující v době změny si uchovají svůj stávající přístup k tématu. Také stávající odběratelé si uchovají svůj přístup k veškerým odběrům, které již provedli.

Aspekty pro fronty aliasů, které se interpretují na témata pro operaci publikování

Při zadání volání MQOPEN nebo MQPUT1 pro frontu aliasů, která je interpretována jako téma, produkt IBM MQ provede dvě kontroly prostředků:

- První z názvů alias fronty určených v deskriptoru objektu (MQOD) v rámci volání MQOPEN nebo MQPUT1 .
- Druhý proti tématu, na které se rozlišuje fronta aliasů

Musíte si být vědomi toho, že toto chování se liší od chování, které dostanete, když se alias fronty vyřeší do jiných front. Potřebujete správný přístup k oběma profilům, abyste mohli pokračovat v akci publikování.

Zabezpečení tématu systému

K následujícím tématům systému je přistupován adresním prostorem inicializátoru kanálu.

ID uživatelů, pod kterými je toto spuštění spuštěno, musí mít přístup k těmto frontám RACF , jak je zobrazeno v Tabulka 42 na stránce 207.

Tabulka 42. Přístup požadovaný pro témata SYSTEM		
Téma SYSTEM	**Profil**	**Inicializátor kanálu pro distribuované fronty**
SYSTEM.BROKER.ADMIN.STREAM	hlq.PUBLISH.topicname	AKTUALIZOVAT
SYSTEM.BROKER.ADMIN.STREAM	hlq.SUBSCRIBE.topicname	ALTER

z/OS *Profily pro procesy*

Je-li zabezpečení procesu aktivní, musíte definovat profily v odpovídajících třídách a povolit k těmto profilům přístup nezbytné skupiny nebo ID uživatelů.

Je-li zabezpečení procesu aktivní, musíte:

- Definujte profily ve třídách **MQPROC** nebo **GMQPROC** , pokud používáte velké profily.
- Definujte profily ve třídách **MXPROC** nebo **GMXPROC** v případě použití smíšených profilů případu.
- Povolte nezbytné skupiny nebo ID uživatelů pro přístup k těmto profilům, aby mohli vydávat požadavky rozhraní API produktu IBM MQ , které používají procesy.

Profily pro procesy mají tvar:

```
hlq.processname
```

kde `hlq` může být buď `qmgr-name` (název správce front), nebo `qsg-name` (název skupiny sdílení front) a `processname` je název procesu, který se otevírá.

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 procesu s tímto názvem ve všech správcích front v rámci skupiny sdílení front. Tento přístup lze potlačit pro jednotlivé správce front definováním profilu úrovně správce front pro danou definici procesu v daném správci front.

Je-li váš správce front členem skupiny sdílení front a používáte-li správce front i zabezpečení na úrovni skupiny sdílení front, produkt IBM MQ nejprve zkontroluje profil s předponou názvu správce front. Pokud ji nenajde, hledá profil s předponou název skupiny sdílení front.

Následující tabulka zobrazuje přístup požadovaný pro otevření procesu.

Tabulka 43. Úrovně přístupu pro zabezpečení procesu

Volba MQOPEN	**Úroveň přístupu produktu RACF je vyžadována pro hlq.processname .**
MQO_ DOTÁZAT SE	READ (čtení)

Například ve správci front MQS9musí být skupina RACF INQVPRC schopna zjistit (`MQINQ`). ve všech procesech začínajících písmenem V. Definice RACF by byly následující:

```
RDEFINE MQPROC MQS9.V* UACC(NONE)
PERMIT MQS9.V* CLASS(MQPROC) ID(INQVPRC) ACCESS(READ)
```

Zabezpečení alternativního uživatele může být také aktivní v závislosti na otevřených volbách, které jsou zadány při otevření objektu definice procesu.

z/OS *Profily pro seznamy názvů*

Je-li zabezpečení seznamu názvů aktivní, definujte profily v příslušných třídách a udělte těmto profilům přístup skupin nebo ID uživatelů.

Je-li zabezpečení seznamu názvů aktivní, musíte:

- Definujte profily ve třídách **MQNLIST** nebo **GMQNLIST** , pokud používáte velké profily.
- Definujte profily ve třídách **MXNLIST** nebo **GMXNLIST** v případě použití smíšených profilů případu.
- Povolte nezbytné skupiny nebo ID uživatelů pro přístup k těmto profilům.

Profily pro seznamy jmen mají tento tvar:

```
hlq.namelistname
```

kde `hlq` může být buď `qmgr-name` (název správce front), nebo `qsg-name` (název skupiny sdílení front) a `namelistname` je název seznamu názvů, který se má otevřít.

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 potlačit pro jednotlivé správce front definováním profilu úrovně správce front pro daný seznam názvů v daném správci front.

Je-li váš správce front členem skupiny sdílení front a používáte-li správce front i zabezpečení na úrovni skupiny sdílení front, produkt IBM MQ nejprve zkontroluje profil s předponou názvu správce front. Pokud ji nenajde, hledá profil s předponou název skupiny sdílení front.

Následující tabulka zobrazuje přístup požadovaný pro otevření seznamu názvů.

Tabulka 44. Úrovně přístupu pro zabezpečení seznamu názvů

Volba MQOPEN	**Úroveň přístupu RACF je vyžadována pro hlq.namelistname .**
MQO_ DOTÁZAT SE	READ (čtení)

Například ve správci front (nebo ve skupině sdílení front) PQM3musí být skupina RACF DEPT571 schopna zjišťovat (`MQINQ`). u těchto seznamů názvů:

- Všechny seznamy názvů začínající na "DEPT571".
- PRINTER/DESTINATIONS/DEPT571
- AGENTURA/ŽÁDOSTI/FRONTY
- WAREHOUSE.BROADCAST

Definice RACF k provedení této akce 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)
```

Alternativní zabezpečení uživatele může být aktivní v závislosti na volbách, které jsou určeny při otevření objektu seznamu názvů.

Zabezpečení seznamu názvů systému

Mnoho systémů jmenovek systému je zpřístupněno pomocnými částmi produktu IBM MQ:

- Obslužný program CSQUTIL
- Ovládací panely a ovládací panely
- Adresní prostor inicializátoru kanálu (včetně démona publikování/odběru zařazeného ve frontě)

ID uživatelů, pod kterými jsou tyto spuštění spuštěny, musí mít RACF přístup k těmto seznamům názvů, jak je zobrazeno v části Tabulka 45 na stránce 209.

Tabulka 45. Přístup k seznamům názvů SYSTEM vyžaduje produkt IBM MQ .

Seznam názvů SYSTEM	**KALKUNIT**	**Ovládací panely a ovládací panely**	**Inicializátor kanálu pro distribuované fronty**
SYSTEM.QPUBSUB.QUEUE.NAMELIST	-	-	READ (čtení)
SYSTEM.QPUBSUB.SUBPOINT.NAMELIST	-	-	READ (čtení)

z/OS *Profily pro alternativní zabezpečení uživatelů*

Je-li zabezpečení alternativního uživatele aktivní, musíte definovat profily v odpovídajících třídách a povolit k těmto profilům přístup nezbytné skupiny nebo ID uživatelů.

Další informace o produktu *`AlternateUserId`*naleznete v části AlternateUserID (MQCHAR12).

Je-li zabezpečení alternativního uživatele aktivní, musíte:

- Definujte profily ve třídách MQADMIN nebo GMQADMIN, používáte-li velké profily.
- Definujte profily ve třídách MXADMIN nebo GMXADMIN, používáte-li smíšené profily případu.

Povolte potřebné skupiny nebo ID uživatelů pro 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 mít následující formát:

```
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 u všech správců front v rámci skupiny sdílení front. Toto alternativní ID uživatele může být použito ve všech správci front v rámci skupiny sdílení front uživatelem, který má správný přístup. Tento přístup lze u jednotlivých správců front potlačit definováním profilu úrovně správce front pro toto alternativní ID uživatele v daném správci front.

Je-li váš správce front členem skupiny sdílení front a používáte-li správce front i zabezpečení na úrovni skupiny sdílení front, produkt IBM MQ nejprve zkontroluje profil s předponou názvu správce front. Pokud ji nenajde, hledá profil s předponou název skupiny sdílení front.

Následující tabulka zobrazuje přístup při zadávání alternativní volby uživatele.

Tabulka 46. Úrovně přístupu pro zabezpečení alternativního uživatele

Volby MQOPEN, MQSUB nebo MQPUT1	**Je vyžadována úroveň přístupu RACF**
MQO_ALTERNATE_USER_AUTHORITY MQSO_ALTERNATE_USER_AUTHORITY MQPMO_ALTERNATE_USER_AUTHORITY	AKTUALIZOVAT

Kromě alternativních kontrol zabezpečení uživatele lze také provést další kontroly zabezpečení pro frontu, proces, seznam názvů a kontext zabezpečení. Alternativní ID uživatele, je-li poskytnuto, se používá pouze pro kontroly zabezpečení ve frontě, definice procesu nebo prostředky seznamu názvů. Pro alternativní kontroly uživatele a zabezpečení kontextu se použije ID uživatele požadující, aby byla kontrola použita. Podrobnosti o tom, jak se zachází s ID uživatele, viz “ID uživatelů pro kontrolu zabezpečení v systému z/OS” na stránce 233. Pro souhrnnou tabulku zobrazující otevřené volby a bezpečnostní kontroly požadované, když jsou všechny aktivní fronty, kontext a alternativní zabezpečení uživatelů, viz Tabulka 36 na stránce 202.

Alternativní uživatelský profil dává požadujícímu ID uživatele přístup k prostředkům přidruženým k ID uživatele uvedenému v alternativním ID uživatele. Například mzdový server spuštěný pod ID uživatele PAYSERV na správci front QMPY zpracovává požadavky od personálních ID uživatelů, přičemž všechny začínají na PS. Chcete-li zajistit, aby práce prováděná serverem mezd byla provedena pod ID uživatele požadujícího uživatele, použije se alternativní oprávnění uživatele. Výplatní server ví, které ID uživatele má být zadáno jako alternativní ID uživatele, protože požadující programy generují zprávy pomocí volby zprávy příkazu MQPMO_DEFAULT_CONTEXT. Další podrobnosti o tom, odkud získáte alternativní ID uživatelů, najdete v tématu “ID uživatelů pro kontrolu zabezpečení v systému z/OS” na stránce 233 .

Následující příklad definice RACF umožňuje programu serveru zadat alternativní ID uživatele 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 při kontrolách profilu, ale pouze prvních 8 bajtů se použije jako ID uživatele pro IBM MQ. Není-li toto oseknutí ID uživatele žádoucí, aplikační programy, které vyžadují požadavek, musí přeložit jakékoli alternativní ID uživatele o více než 8 bajtů do něčeho vhodnějšího.
2. Uvedete-li MQO_ALTERNATE_USER_AUTHORITY, MQSO_ALTERNATE_USER_AUTHORITY nebo MQPMO_ALTERNATE_USER_AUTHORITY a nezadáte do deskriptoru objektu pole *AlternateUserId* , použije se ID uživatele mezery. Pro účely alternativního zabezpečení uživatele zkontrolujte, zda 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 provedou s ID uživatele, které je prázdné. Podrobnosti o prázdných ID uživatelů najdete v tématu "Prázdné ID uživatele a úrovně UACC" na stránce 241.

Správa alternativních ID uživatelů je snazší, máte-li konvence pojmenování pro ID uživatelů, která vám umožní používat generické alternativní uživatelské profily. Pokud tomu tak není, můžete použít funkci RACVARS produktu RACF . Podrobnosti o používání RACVARS najdete v příručce *z/OS SecureWay Security Server RACF Security Administrator's Guide*.

Je-li zpráva vložena do fronty, která byla otevřena s alternativním oprávněním uživatele a kontext zprávy byl vygenerován správcem front, je pole MQMD_USER_IDENTIFIER nastaveno na alternativní ID uživatele.

z/OS *Profily pro zabezpečení kontextu*

Je-li zabezpečení kontextu aktivní, chcete-li řídit přístup k informacím o kontextu zpráv, musíte definovat profily v odpovídajících třídách a povolit k těmto profilům přístup nezbytné skupiny nebo ID uživatelů. Kontext zprávy je obsažen v deskriptoru zpráv (MQMD).

Použití profilů pro zabezpečení kontextu

Je-li zabezpečení kontextu aktivní, chcete-li uživatelům povolit přístup ke kontextovým informacím pro zprávy v určité frontě nebo při publikování do určitého tématu, musíte definovat profil v jedné z následujících tříd:

- Třída `MQADMIN` , pokud používáte velké profily.
- Třída `MXADMIN` v případě použití smíšených profilů velkých a malých písmen.

Profily pro zabezpečení kontextu mohou být uvedeny na úrovni subsystému nebo na úrovni skupiny sdílení front a mají následující tvar:

```
hlq.CONTEXT.queuename
hlq.CONTEXT.topicname
```

kde *hlq* může být buď název správce front, nebo název skupiny sdílení front a *název_fronty* a *název_tématu* může být buď úplný, nebo generický název fronty nebo tématu, pro které chcete definovat profil kontextu.

Profil s předponou s názvem správce front a s názvem ** určeným jako název fronty nebo tématu umožňuje řízení kontextu zabezpečení kontextu ve všech frontách a tématech náležejících tomuto správci front. Toto lze potlačit pro jednotlivé fronty nebo téma definováním specifického profilu pro kontext v dané frontě nebo tématu.

Profil s předponou názvu skupiny sdílení front a s názvem ** určeným jako název fronty nebo tématu umožňuje řízení kontextu ve všech frontách a tématech náležejících ke správcům front v rámci skupiny sdílení front. Tento stav lze u jednotlivých správců front přepsat definováním profilu úrovně správce front pro kontext v daném správci front zadáním profilu s předponou názvu správce front. Lze ji také přepsat v jednotlivé frontě nebo tématu zadáním přípony profilu s názvem fronty nebo tématu.

Je-li váš správce front členem skupiny sdílení front a používáte-li správce front i zabezpečení na úrovni skupiny sdílení front, produkt IBM MQ nejprve zkontroluje profil s předponou názvu správce front. Pokud ji nenajde, hledá profil s předponou název skupiny sdílení front.

Musíte povolit potřebné skupiny nebo ID uživatelů pro přístup k tomuto profilu. Následující tabulka zobrazuje požadovanou úroveň přístupu v závislosti na specifikaci kontextových voleb při otevření fronty.

Tabulka 47. Úrovně přístupu pro zabezpečení kontextu	
Volba MQOPEN nebo MQPUT1	**Úroveň přístupu produktu RACF je vyžadována pro hlq.CONTEXT.queuename nebo hlq.CONTEXT.topicname .**
MQPMOTO_NE_KONTEXT	Žádná kontrola zabezpečení kontextu
MQPMO_VÝCHOZÍ_KONTEXT	Žádná kontrola zabezpečení kontextu
ÁLNÍ_KONTEXT 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
MQO_SET_ALL_CONTEXT MQPMO_SET_ALL_CONTEXT	CONTROL
MQOO_OUTPUT nebo MQPUT1(POUŽITÍ (XMITQ))	CONTROL
Volba MQSUB	
MQSO_SET_IDENTITY_CONTEXT **(Poznámka 2)**	AKTUALIZOVAT

Poznámka:

1. ID uživatelů použitá pro distribuované ukládání do fronty vyžadují k umístění zpráv do cílové fronty přístup CONTROL ke správci `hlq.CONTEXT.queuename` . Chcete-li získat informace o použitých ID uživatelů, prohlédněte si příručku “ID uživatele použitá inicializátorem kanálu” na stránce 236 .
2. Pokud v požadavku MQSUB s uvedenými volbami MQSO_CREATE nebo MQSO_ALTER chcete nastavit kterékoli z polí kontextu identity ve struktuře MQSD, je třeba určit volbu MQSO_SET_IDENTITY_CONTEXT. Požadujete také odpovídající oprávnění ke kontextovému profilu pro cílovou frontu.

Pokud příkazy vložíte do vstupní fronty příkazů systému, použijte k přidružení správného ID uživatele k příkazu výchozí kontextovou volbu pro zprávu.

Například obslužný program dodaný IBM MQCSQUTIL může být použit k odlehčování a opětnému načtení zpráv ve frontách. Jsou-li odložené zprávy obnoveny do fronty, obslužný program CSQUTIL použije volbu MQOO_SET_ALL_CONTEXT k vrácení zpráv do původního stavu. Kromě zabezpečení fronty, které je vyžadováno touto volbou otevření, je také vyžadováno oprávnění ke kontextu. Je-li například toto oprávnění vyžadováno skupinou BACKGRP ve správci front MQS1, bude to definováno následujícím způsobem:

```
RDEFINE MQADMIN MQS1.CONTEXT.** UACC(NONE)
PERMIT MQS1.CONTEXT.** CLASS(MQADMIN) ID(BACKGRP) ACCESS(CONTROL)
```

V závislosti na uvedených volbách a typech provedených zabezpečení se při otevření fronty mohou vyskytnout i jiné typy kontrol zabezpečení. Patří k nim zabezpečení fronty (viz “Profily pro zabezpečení fronty” na stránce 194) a alternativní zabezpečení uživatelů (viz “Profily pro alternativní zabezpečení uživatelů” na stránce 209). Pro souhrnnou tabulku zobrazující otevřené volby a bezpečnostní kontroly požadované, když jsou všechny aktivní fronty, kontext a alternativní zabezpečení uživatelů, viz Tabulka 36 na stránce 202.

Zabezpečení kontextu systémové fronty

K mnoha systémovým frontám je přistupováno pomocnými částmi produktu IBM MQ, například adresním prostorem inicializátoru kanálu a serverem mqweb využívaným produkty IBM MQ Console a REST API.

ID uživatelů, pod kterými tyto úlohy běží, musí mít přístup k těmto frontám RACF , jak je zobrazeno v Tabulka 48 na stránce 213.

Tabulka 48. Přístup požadovaný k frontám SYSTEM pro operace kontextu

Fronta SYSTEM	**Inicializátor kanálu pro distribuované fronty**	**mqweb server**
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 kontrolují příkazy MQSC a PCF. Profily lze použít pro správce front nebo skupinu sdílení front.

Chcete-li zkontrolovat zabezpečení příkazů (takže jste nedefinovali profil přepínačů zabezpečení příkazu hlq.NO.CMD.CHECKS), musíte přidat profily do třídy MQCMDS.

Tytéž profily zabezpečení řídí příkazy MQSC a PCF. Názvy profilů produktu RACF pro kontrolu zabezpečení příkazů jsou založeny na 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 sloveso část názvu příkazu, například ALTER, a `pkw` je typ objektu, například QLOCAL pro lokální frontu.

Proto je název profilu pro příkaz ALTER QLOCAL v subsystému CSQ1 následující:

```
CSQ1.ALTER.QLOCAL
```

Generické profily můžete použít k ochraně sad příkazů tak, abyste měli méně profilů k údržbě, a tedy méně seznamů pro přístup. Zvažte vytvoření generického profilu, který platí pro všechny příkazy, které nejsou chráněné specifičtěji profilem. Definujte tento profil pomocí UACC (NONE) a udělte přístup ALTER pouze ke skupinám RACF , které obsahují administrátory. Pak můžete vytvořit generický profil použitelný pro všechny příkazy DISPLAY a udělit rozšířený přístup k němu. Mezi těmito extrémy můžete identifikovat skupiny uživatelů, kteří potřebují přístup k určitým sadám příkazů. V takovém případě můžete vytvářet profily pro tyto sady a udělit přístup skupinám uživatelů RACF zastupujícím tyto třídy uživatelů. Vyhněte se tomu, aby uživatelé měli přístup k příkazům, které nevyžadují: Použijte zásadu alespoň oprávnění, aby měli uživatelé přístup pouze k příkazům, které jsou vyžadovány pro jejich úlohy.

Profil s předponou názvu správce front řídí použití tohoto příkazu v daném správci front. Profil s předponou názvu skupiny sdílení front řídí použití příkazu ve všech správcích front v rámci skupiny sdílení front. Tento přístup lze u jednotlivých správců front potlačit definováním profilu úrovně správce front pro daný příkaz v daném správci front.

Je-li váš správce front členem skupiny sdílení front a používáte-li správce front i zabezpečení na úrovni skupiny sdílení front, produkt IBM MQ vyhledá předponu s předponou názvu správce front. Pokud ji nenajde, hledá profil s předponou název skupiny sdílení front.

Nastavením profilů příkazů na úrovni správce front může být uživatel omezen na vydávání příkazů v konkrétním správci front. Případně můžete definovat jeden profil pro skupinu sdílení front pro každé příkazové slovo a všechny kontroly zabezpečení se místo jednotlivých správců front budou provádět s tímto profilem.

Je-li zabezpečení subsystému i zabezpečení skupiny sdílení front aktivní a lokální profil není nalezen, provede se kontrola zabezpečení příkazu, zda má uživatel přístup k profilu skupiny sdílení front.

Pokud použijete atribut CMDSCOPE pro směrování příkazu do jiných správců front ve skupině sdílení front, je kontrolováno každého správce front, ve kterém je příkaz spuštěn, ale nemusí být nutně ve správci front, ve kterém je zadán příkaz.

Tabulka 49 na stránce 214 zobrazuje pro každý příkaz IBM MQ MQSC profily vyžadované pro kontrolu zabezpečení příkazu a odpovídající úroveň přístupu pro každý profil ve třídě MQCMDS.

Tabulka 50 na stránce 220 zobrazuje pro každý příkaz IBM MQ PCF profily nezbytné pro kontrolu zabezpečení příkazů 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 prostředků příkazů pro MQADMIN nebo MXADMIN**	**Úroveň přístupu pro MQADMIN nebo MXADMIN**
ZMĚNIT AUTHINFO	hlq.ALTER.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
ZMĚNIT FOND VYROVNÁVACÍCH PAMĚTÍ	hlq.ALTER.BUFFPOOL	ALTER	Žádná kontrola	-
ZMĚNIT CFSTRUCT	hlq.ALTER.CFSTRUCT	ALTER	Žádná kontrola	-
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
POZMĚNIT PSID	hlq.ALTER.PSID	ALTER	Žádná kontrola	-
ZMĚNIT ALIAS QALIAS	hlq.ALTER.QALIAS	ALTER	hlq.QUEUE.queue	ALTER
POZMĚNIT QLOCAL	hlq.ALTER.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
ZMĚNIT QMGR	hlq.ALTER.QMGR	ALTER	Žádná kontrola	-
ZMĚNIT MODEL QMODEL	hlq.ALTER.QMODEL	ALTER	hlq.QUEUE.queue	ALTER
ZMĚNIT QREMOTE	hlq.ALTER.QREMOTE	ALTER	hlq.QUEUE.queue	ALTER
POZMĚNIT ZABEZPEČENÍ	hlq.ALTER.SECURITY	ALTER	Žádná kontrola	-
POZMĚNIT SMDS	hlq.ALTER.SMDS	ALTER	Žádná kontrola	-

Tabulka 49. Příkazy MQSC, profily a jejich úrovně přístupu (pokračování)

Příkaz	Profil příkazu pro MQCMDS	Úroveň přístupu pro MQCMDS	Profil prostředků příkazů pro MQADMIN nebo MXADMIN	Úroveň přístupu pro MQADMIN nebo MXADMIN
ZMĚNIT TŘÍDU STGCLASS	hlq.ALTER.STGCLASS	ALTER	Žádná kontrola	-
ZMĚNIT DÍLČÍ	hlq.ALTER.SUB	ALTER	Žádná kontrola	-
ALTER TOPIC	hlq.ALTER.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
ZMĚNIT TRASOVÁNÍ	hlq.ALTER.TRACE	ALTER	Žádná kontrola	-
PROTOKOL ARCHIVACE	hlq.ARCHIVE.LOG	CONTROL	Žádná kontrola	-
ZÁLOŽNÍ FSTRUCT	hlq.BACKUP.CFSTRUCT	CONTROL	Žádná kontrola	-
VYMAZAT QLOCAL	hlq.CLEAR.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
CLEAR TOPICSTR “3” na stránce 220	hlq.CLEAR.TOPICSTR	ALTER	hlq.TOPIC.topic	ALTER
DEFINOVAT AUTHINFO	hlq.DEFINE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
DEFINOVAT FOND VYROVNÁVACÍCH PAMĚTÍ	hlq.DEFINE.BUFFPOOL	ALTER	Žádná kontrola	-
DEFINOVAT CFSTRUCT	hlq.DEFINE.CFSTRUCT	ALTER	Žádná kontrola	-
Definovat kanál	hlq.DEFINE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
DEFINOVAT PROTOKOL	hlq.DEFINE.LOG	ALTER	Žádná kontrola	-
DEFINOVAT HODNOTY MAXSMSGS	hlq.DEFINE.MAXSMSGS	ALTER	Žádná kontrola	-
DEFINOVAT SEZNAM NÁZVŮ	hlq.DEFINE.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
DEFINOVÁNÍ PROCESU	hlq.DEFINE.PROCESS	ALTER	hlq.PROCESS.process	ALTER
DEFINOVAT PSID	hlq.DEFINE.PSID	ALTER	Žádná kontrola	-
DEFINOVAT ALIAS QALIAS	hlq.DEFINE.QALIAS	ALTER	hlq.QUEUE.queue	ALTER
DEFINOVAT QLOCAL	hlq.DEFINE.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
DEFINOVAT MODEL QMODEL	hlq.DEFINE.QMODEL	ALTER	hlq.QUEUE.queue	ALTER
DEFINOVAT QREMOTE	hlq.DEFINE.QREMOTE	ALTER	hlq.QUEUE.queue	ALTER
DEFINOVAT TŘÍDU STGCLASS	hlq.DEFINE.STGCLASS	ALTER	Žádná kontrola	-

Tabulka 49. Příkazy MQSC, profily a jejich úrovně přístupu (pokračování)

Příkaz	Profil příkazu pro MQCMDS	Úroveň přístupu pro MQCMDS	Profil prostředků příkazů pro MQADMIN nebo MXADMIN	Úroveň přístupu pro MQADMIN nebo MXADMIN
DEFINE SUB	hlq.DEFINE.SUB	ALTER	Žádná kontrola	-
DEFINOVAT TÉMA	hlq.DEFINE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
ODSTRANIT AUTHINFO	hlq.DELETE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
ODSTRANIT FOND VYROVNÁVACÍCH PAMĚTÍ	hlq.DELETE.BUFFPOOL	ALTER	Žádná kontrola	-
ODSTRANIT CFSTRUCT	hlq.DELETE.CFSTRUCT	ALTER	Žádná kontrola	-
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	Žádná kontrola	-
ODSTRANIT ALIAS QALIAS	hlq.DELETE.QALIAS	ALTER	hlq.QUEUE.queue	ALTER
ODSTRANIT QLOCAL	hlq.DELETE.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
ODSTRANIT MODEL QMODEL	hlq.DELETE.QMODEL	ALTER	hlq.QUEUE.queue	ALTER
ODSTRANIT QREMOTE	hlq.DELETE.QREMOTE	ALTER	hlq.QUEUE.queue	ALTER
ODSTRANIT STGCLASS	hlq.DELETE.STGCLASS	ALTER	Žádná kontrola	-
ODSTRANIT DÍLČÍ	hlq.DELETE.SUB	ALTER	Žádná kontrola	-
Odstranit téma	hlq.DELETE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
“1” na stránce 220 ARCHIVACE	hlq.DISPLAY.ARCHIVE	READ (čtení)	Žádná kontrola	-
ZOBRAZIT AUTHINFO	hlq.DISPLAY.AUTHINFO	READ (čtení)	Žádná kontrola	-
ZOBRAZIT STAV CFSTATUS	hlq.DISPLAY.CFSTATUS	READ (čtení)	Žádná kontrola	-
ZOBRAZIT CFSTRUCT	hlq.DISPLAY.CFSTRUCT	READ (čtení)	Žádná kontrola	-
ZOBRAZIT KANÁL	hlq.DISPLAY.CHANNEL	READ (čtení)	Žádná kontrola	-
ZOBRAZIT CHINIT	hlq.DISPLAY.CHINIT	READ (čtení)	Žádná kontrola	-

Tabulka 49. Příkazy MQSC, profily a jejich úrovně přístupu (pokračování)

Příkaz	Profil příkazu pro MQCMDS	Úroveň přístupu pro MQCMDS	Profil prostředků příkazů pro MQADMIN nebo MXADMIN	Úroveň přístupu pro MQADMIN nebo MXADMIN
ZOBRAZIT VELIKOST CHUSH	hlq.DISPLAY.CHLAUTH	READ (čtení)	Žádná kontrola	-
ZOBRAZIT STAV CHSTATUS	hlq.DISPLAY.CHSTATUS	READ (čtení)	Žádná kontrola	-
ZOBRAZIT CLUQMGR	hlq.DISPLAY.CLUSQMGR	READ (čtení)	Žádná kontrola	-
ZOBRAZIT CMDSERV	hlq.DISPLAY.CMDSERV	READ (čtení)	Žádná kontrola	-
DISPLAY CONN “1” na stránce 220	hlq.DISPLAY.CONN	READ (čtení)	Žádná kontrola	-
Zobrazit skupinu	hlq.DISPLAY.GROUP	READ (čtení)	Žádná kontrola	-
DISPLAY LOG “1” na stránce 220	hlq.DISPLAY.LOG	READ (čtení)	Žádná kontrola	-
ZOBRAZIT VLASTNOSTI MAXSMSGS	hlq.DISPLAY.MAXSMSGS	READ (čtení)	Žádná kontrola	-
ZOBRAZIT SEZNAM NÁZVŮ	hlq.DISPLAY.NAMELIST	READ (čtení)	Žádná kontrola	-
ZOBRAZIT PROCES	hlq.DISPLAY.PROCESS	READ (čtení)	Žádná kontrola	-
ZOBRAZIT PUBSUB	hlq.DISPLAY.PUBSUB	READ (čtení)	Žádná kontrola	-
ZOBRAZIT ALIAS QALIAS	hlq.DISPLAY.QALIAS	READ (čtení)	Žádná kontrola	-
ZOBRAZIT QCLUSTER	hlq.DISPLAY.QCLUSTER	READ (čtení)	Žádná kontrola	-
ZOBRAZIT QLOCAL	hlq.DISPLAY.QLOCAL	READ (čtení)	Žádná kontrola	-
ZOBRAZIT QMGR	hlq.DISPLAY.QMGR	READ (čtení)	Žádná kontrola	-
ZOBRAZIT MODEL QMODEL	hlq.DISPLAY.QMODEL	READ (čtení)	Žádná kontrola	-
ZOBRAZIT QREMOTE	hlq.DISPLAY.QREMOTE	READ (čtení)	Žádná kontrola	-
ZOBRAZIT STAV QSTATUS	hlq.DISPLAY.QSTATUS	READ (čtení)	Žádná kontrola	-

Tabulka 49. Příkazy MQSC, profily a jejich úrovně přístupu (pokračování)

Příkaz	Profil příkazu pro MQCMDS	Úroveň přístupu pro MQCMDS	Profil prostředků příkazů pro MQADMIN nebo MXADMIN	Úroveň přístupu pro MQADMIN nebo MXADMIN
ZOBRAZIT FRONTU	hlq.DISPLAY.QUEUE	READ (čtení)	Žádná kontrola	-
ZOBRAZIT STAV SBSTATUS	hlq.DISPLAY.SBSTATUS	READ (čtení)	Žádná kontrola	-
Zobrazit sadu SMDS	hlq.DISPLAY.SMDS	READ (čtení)	Žádná kontrola	-
ZOBRAZIT PŘIPOJENÍ SMDSCONN	hlq.DISPLAY.SMDSCONN	READ (čtení)	Žádná kontrola	-
ZOBRAZIT POD	hlq.DISPLAY.SUB	READ (čtení)	Žádná kontrola	-
ZOBRAZIT ZABEZPEČENÍ	hlq.DISPLAY.SECURITY	READ (čtení)	Žádná kontrola	-
ZOBRAZIT TŘÍDU STGCLASS	hlq.DISPLAY.STGCLASS	READ (čtení)	Žádná kontrola	-
SYSTÉM DISPLAY “1” na stránce 220	hlq.DISPLAY.SYSTEM	READ (čtení)	Žádná kontrola	-
ZOBRAZIT VLÁKNO	hlq.DISPLAY.THREAD	READ (čtení)	Žádná kontrola	-
ZOBRAZIT STAV TPSTATUS	hlq.DISPLAY.TPSTATUS	READ (čtení)	Žádná kontrola	-
ZOBRAZIT TÉMA	hlq.DISPLAY.TOPIC	READ (čtení)	Žádná kontrola	-
ZOBRAZIT STAV TPSTATUS	hlq.DISPLAY.TPSTATUS	READ (čtení)	Žádná kontrola	-
ZOBRAZIT TRASOVÁNÍ	hlq.DISPLAY.TRACE	READ (čtení)	Žádná kontrola	-
Zobrazení využití“1” na stránce 220	hlq.DISPLAY.USAGE	READ (čtení)	Žádná kontrola	-
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	Žádná kontrola	-
OBNOVIT CFSTRUCT	hlq.RECOVER.CFSTRUCT	CONTROL	Žádná kontrola	-
Aktualizovat klastr	hlq.REFRESH.CLUSTER	ALTER	Žádná kontrola	-
AKTUALIZOVAT SPRÁVCE FRONT	hlq.REFRESH.QMGR	ALTER	Žádná kontrola	-

Tabulka 49. Příkazy MQSC, profily a jejich úrovně přístupu (pokračování)

Příkaz	Profil příkazu pro MQCMDS	Úroveň přístupu pro MQCMDS	Profil prostředků příkazů pro MQADMIN nebo MXADMIN	Úroveň přístupu pro MQADMIN nebo MXADMIN
REFRESH SECURITY	hlq.REFRESH.SECURITY	ALTER	Žádná kontrola	-
RESETOVAT CFSTRUCT	hlq.RESET.CFSTRUCT	CONTROL	Žádná kontrola	-
Resetovat kanál	hlq.RESET.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Reset klastru	hlq.RESET.CLUSTER	CONTROL	Žádná kontrola	-
RESETOVAT QMGR	hlq.RESET.QMGR	CONTROL	Žádná kontrola	-
RESETOVAT QSTATS	hlq.RESET.QSTATS	CONTROL	hlq.QUEUE.queue	CONTROL
Resetovat SMDS	hlq.RESET.SMDS	CONTROL	Žádná kontrola	-
Obnovit položku Tpipe	hlq.RESET.TPIPE	CONTROL	Žádná kontrola	-
Vyřešit kanál	hlq.RESOLVE.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Vyřešit nejisté položky	hlq.RESOLVE.INDOUBT	CONTROL	Žádná kontrola	-
OBNOVIT SPRÁVCE FRONT	hlq.RESUME.QMGR	CONTROL	Žádná kontrola	-
ZABEZPEČENÍ OVĚŘENÍ	hlq.RVERIFY.SECURITY	ALTER	Žádná kontrola	-
Nastavit archiv	hlq.SET.ARCHIVE	CONTROL	Žádná kontrola	-
SET CHLAUTH	hlq.SET.CHLAUTH	CONTROL	Žádná kontrola	-
Nastavit protokol	hlq.SET.LOG	CONTROL	Žádná kontrola	-
Nastavit systém	hlq.SET.SYSTEM	CONTROL	Žádná kontrola	-
Spustit kanál	hlq.START.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
START CHINIT “4” na stránce 220	hlq.START.CHINIT	CONTROL	Žádná kontrola	-
SPUSTIT CMDSERV	hlq.START.CMDSERV	CONTROL	Žádná kontrola	-
Spustit listener	hlq.START.LISTENER	CONTROL	Žádná kontrola	-
SPUSTIT SPRÁVCE FRONT	Není“2” na stránce 220	-	-	-
SPUSTIT PŘÍKAZ SMDSCONN	hlq.START.SMDSCONN	CONTROL	Žádná kontrola	-
Spustit trasování	hlq.START.TRACE	CONTROL	Žádná kontrola	-
Ukončit kanál	hlq.STOP.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
UKONČIT CHINIT	hlq.STOP.CHINIT	CONTROL	Žádná kontrola	-
UKONČIT CMDSERV	hlq.STOP.CMDSERV	CONTROL	Žádná kontrola	-
Ukončit listener	hlq.STOP.LISTENER	CONTROL	Žádná kontrola	-

Tabulka 49. Příkazy MQSC, profily a jejich úrovně přístupu (pokračování)				
Příkaz	**Profil příkazu pro MQCMDS**	**Úroveň přístupu pro MQCMDS**	**Profil prostředků příkazů pro MQADMIN nebo MXADMIN**	**Úroveň přístupu pro MQADMIN nebo MXADMIN**
ZASTAVIT QMGR	hlq.STOP.QMGR	CONTROL	Žádná kontrola	-
ZASTAVIT PŘÍKAZ SMDSCONN	hlq.STOP.SMDSCONN	CONTROL	Žádná kontrola	-
Zastavit trasování	hlq.STOP.TRACE	CONTROL	Žádná kontrola	-
SUSPEND QMgr	hlq.SUSPEND.QMGR	CONTROL	Žádná kontrola	-

Notes:

1. Tyto příkazy mohou být vydávány interně správcem front; v těchto případech se nekontroluje žádná oprávnění.
2. IBM MQ nekontroluje oprávnění uživatele, který vydává příkaz START QMGR. Můžete však použít produkt RACFnebo alternativní zařízení zabezpečení k řízení přístupu k příkazu START xxxxMSTR , který je vydán jako výsledek příkazu START QMGR. To se provádí řízením přístupu k profilu MVS.START.STC.xxxxMSTR ve třídě operátorů operátorů RACF (OPERCMDS). Podrobné informace o této proceduře naleznete v příručce *z/OS SecureWay Security Server RACF Security Administrator's Guide*. Použijete-li tuto techniku a neautorizovaný uživatel se pokusí spustit správce front, bude ukončen s kódem příčiny 00F30216.
3. Prostředek **hlq.TOPIC.topic** se odkazuje na objekt Topic odvozený z TOPCSTR. Další informace viz “Zabezpečení publikování/odběru” na stránce 473
4. Ve vydáních před verzí IBM MQ for z/OS V6byla kontrola zabezpečení pro MVS.START.STC.CSQ1CHIN. Ve verzi IBM MQ for z/OS V6 a vyšší má k názvu prostředku k sobě přidán další kvalifikátor JOBNAME. To může způsobit problémy při spouštění inicializátoru kanálu.

   Chcete-li vyřešit problém, nahraďte 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 z/OS produktová dokumentace pro *Plánování operací, Příkazy MVS, přístupové autority RACF a názvy prostředků*.

   Příkaz START pro *ssid* MSTR nezahrnuje parametr JOBNAME=. V zájmu konzistence možná budete chtít aktualizovat profil pro MVS.START.STC.ssidMSTR na MVS.START.STC.ssidMSTR. *.

Tabulka 50. PCF příkazy, profily a jejich úrovně přístupu				
Příkaz	**Profil příkazu pro MQCMDS**	**Úroveň přístupu pro MQCMDS**	**Profil prostředků příkazů pro MQADMIN nebo MXADMIN**	**Úroveň přístupu pro MQADMIN nebo MXADMIN**
Zálohovat strukturu CF	hlq.BACKUP.CFSTRUCT	CONTROL	Žádná kontrola	-
Změnit objekt ověřovacích informací	hlq.ALTER.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
Změnit strukturu CF	hlq.ALTER.CFSTRUCT	ALTER	Žádná kontrola	-
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

Tabulka 50. PCF příkazy, profily a jejich úrovně přístupu (pokračování)

Příkaz	Profil příkazu pro MQCMDS	Úroveň přístupu pro MQCMDS	Profil prostředků příkazů pro MQADMIN nebo MXADMIN	Úroveň přístupu pro MQADMIN nebo MXADMIN
Změnit frontu	hlq.ALTER.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
Změnit správce front	hlq.ALTER.QMGR	ALTER	Žádná kontrola	-
Změna zabezpečení	hlq.ALTER.SECURITY	ALTER	Žádná kontrola	-
Změnit SMDS	hlq.ALTER.SMDS	ALTER	Žádná kontrola	-
Změnit úložnou třídu	hlq.ALTER.STGCLASS	ALTER	Žádná kontrola	-
Změnit odběr	hlq.ALTER.SUB	ALTER	Žádná kontrola	-
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 224	hlq.CLEAR.TOPICSTR	ALTER	hlq.TOPIC.topic	ALTER
Kopírování objektu ověřovacích informací	hlq.DEFINE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
Kopírovat strukturu CF	hlq.DEFINE.CFSTRUCT	ALTER	Žádná kontrola	-
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	Žádná kontrola	-
Kopírovat úložnou třídu	hlq.DEFINE.STGCLASS	ALTER	Žádná kontrola	-
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	Žádná kontrola	-
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	hlq.DEFINE.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
Vytvořit úložnou třídu	hlq.DEFINE.STGCLASS	ALTER	Žádná kontrola	-
Vytvořit odběr	hlq.DEFINE.SUB	ALTER	Žádná kontrola	-
Vytvořit téma	hlq.DEFINE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
Odstranit objekt ověřovacích informací	hlq.DELETE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
Odstranit strukturu CF	hlq.DELETE.CFSTRUCT	ALTER	Žádná kontrola	-
Odstranit kanál	hlq.DELETE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
Odstranit seznam názvů	hlq.DELETE.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER

Tabulka 50. PCF příkazy, profily a jejich úrovně přístupu (pokračování)

Příkaz	Profil příkazu pro MQCMDS	Úroveň přístupu pro MQCMDS	Profil prostředků příkazů pro MQADMIN nebo MXADMIN	Úroveň přístupu pro MQADMIN nebo MXADMIN
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	Žádná kontrola	-
Odstranit odběr	hlq.DELETE.SUB	ALTER	Žádná kontrola	-
Odstranit téma	hlq.DELETE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
Zjistit archiv	hlq.DISPLAY.ARCHIVE	READ (čtení)	Žádná kontrola	-
Zjistit objekt ověřovacích informací	hlq.DISPLAY.AUTHINFO	READ (čtení)	Žádná kontrola	-
Zjišťovat názvy objektů ověřovacích informací	hlq.DISPLAY.AUTHINFO	READ (čtení)	Žádná kontrola	-
Zjistit strukturu CF	hlq.DISPLAY.CFSTRUCT	READ (čtení)	Žádná kontrola	-
Zjistit názvy struktury CF	hlq.DISPLAY.CFSTRUCT	READ (čtení)	Žádná kontrola	-
Zjistit stav struktury CF	hlq.DISPLAY.CFSTATUS	READ (čtení)	Žádná kontrola	-
Zjistit kanál	hlq.DISPLAY.CHANNEL	READ (čtení)	Žádná kontrola	-
Zjistit záznam ověření kanálu	hlq.DISPLAY.CHLAUTH	READ (čtení)	Žádná kontrola	-
Zjistit inicializátor kanálu	hlq.DISPLAY.CHINIT	READ (čtení)	Žádná kontrola	-
Zjistit názvy kanálů	hlq.DISPLAY.CHANNEL	READ (čtení)	Žádná kontrola	-
Zjistit stav kanálu	hlq.DISPLAY.CHSTATUS	READ (čtení)	Žádná kontrola	-
Zjistit správce front klastru	hlq.DISPLAY.CLUSQMGR	READ (čtení)	Žádná kontrola	-
Zjistit připojení	hlq.DISPLAY.CONNPCF	READ (čtení)	Žádná kontrola	-
Zjišťovat skupinu	hlq.DISPLAY.GROUP	READ (čtení)	Žádná kontrola	-
Zjistit protokol	hlq.DISPLAY.LOG	READ (čtení)	Žádná kontrola	-
Zjistit seznam názvů	hlq.DISPLAY.NAMELIST	READ (čtení)	Žádná kontrola	-
Zjistit názvy seznamů názvů	hlq.DISPLAY.NAMELIST	READ (čtení)	Žádná kontrola	-
Zjistit proces	hlq.DISPLAY.PROCESS	READ (čtení)	Žádná kontrola	-
Zjistit názvy procesů	hlq.DISPLAY.PROCESS	READ (čtení)	Žádná kontrola	-
Zjistit stav publikování/ odběru	hlq.DISPLAY.PUBSUB	READ (čtení)	Žádná kontrola	-
Zjistit frontu	hlq.DISPLAY.QUEUE	READ (čtení)	Žádná kontrola	-
Zjistit správce front	hlq.DISPLAY.QMGR	READ (čtení)	Žádná kontrola	-
Zjistit názvy front	hlq.DISPLAY.QUEUE	READ (čtení)	Žádná kontrola	-
Zjistit stav fronty	hlq.DISPLAY.QSTATUS	READ (čtení)	Žádná kontrola	-
Zjistit zabezpečení	hlq.DISPLAY.SECURITY	READ (čtení)	Žádná kontrola	-
Zjistit SMDS	hlq.DISPLAY.SMDS	READ (čtení)	Žádná kontrola	-

Tabulka 50. PCF příkazy, profily a jejich úrovně přístupu (pokračování)

Příkaz	Profil příkazu pro MQCMDS	Úroveň přístupu pro MQCMDS	Profil prostředků příkazů pro MQADMIN nebo MXADMIN	Úroveň přístupu pro MQADMIN nebo MXADMIN
Zjistit SMDSCONN	hlq.DISPLAY.SMDSCONN	READ (čtení)	Žádná kontrola	-
Zjistit úložnou třídu	hlq.DISPLAY.STGCLASS	READ (čtení)	Žádná kontrola	-
Zjistit názvy úložné třídy	hlq.DISPLAY.STGCLASS	READ (čtení)	Žádná kontrola	-
Zjistit odběr	hlq.INQUIRE.SUB	READ (čtení)	Žádná kontrola	-
Zjistit stav odběru	hlq.INQUIRE.SBSTATUS	READ (čtení)	Žádná kontrola	-
Zjistit systém	hlq.DISPLAY.SYSTEM	READ (čtení)	Žádná kontrola	-
Zjistit téma	hlq.DISPLAY.TOPIC	READ (čtení)	Žádná kontrola	-
Zjistit názvy témat	hlq.DISPLAY.TOPIC	READ (čtení)	Žádná kontrola	-
Zjistit stav tématu	hlq.DISPLAY.TPSTATUS	READ (čtení)	Žádná kontrola	-
Zjistit použití	hlq.DISPLAY.USAGE	READ (čtení)	Žádná kontrola	-
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	Žádná kontrola	-
Aktualizovat klastr	hlq.REFRESH.CLUSTER	ALTER	Žádná kontrola	-
Aktualizovat správce front	hlq.REFRESH.QMGR	ALTER	Žádná kontrola	-
Aktualizovat zabezpečení	hlq.REFRESH.SECURITY	ALTER	Žádná kontrola	-
Resetovat strukturu CF	hlq.RESET.CFSTRUCT	CONTROL	Žádná kontrola	-
Resetovat kanál	hlq.RESET.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Reset klastru	hlq.RESET.CLUSTER	CONTROL	Žádná kontrola	-
Obnovit správce front	hlq.RESET.QMGR	CONTROL	Žádná kontrola	-
Obnovit statistiku front	hlq.RESET.QSTATS	CONTROL	hlq.QUEUE.queue	CONTROL
Resetovat SMDS	hlq.RESET.SMDS	CONTROL	Žádná kontrola	-
Vyřešit kanál	hlq.RESOLVE.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Obnovit správce front	hlq.RESUME.QMGR	CONTROL	Žádná kontrola	-
Obnovit klastr správců front	hlq.RESUME.QMGR	CONTROL	Žádná kontrola	-
Znovu ověřit zabezpečení	hlq.RVERIFY.SECURITY	ALTER	Žádná kontrola	-
Nastavit archiv	hlq.SET.ARCHIVE	CONTROL	Žádná kontrola	-
Nastavit záznam ověření kanálu	hlq.SET.CHLAUTH	CONTROL	Žádná kontrola	-
Nastavit protokol	hlq.SET.LOG	CONTROL	Žádná kontrola	-
Nastavit systém	hlq.SET.SYSTEM	CONTROL	Žádná kontrola	-
Spustit kanál	hlq.START.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL

Tabulka 50. PCF příkazy, profily a jejich úrovně přístupu (pokračování)				
Příkaz	**Profil příkazu pro MQCMDS**	**Úroveň přístupu pro MQCMDS**	**Profil prostředků příkazů pro MQADMIN nebo MXADMIN**	**Úroveň přístupu pro MQADMIN nebo MXADMIN**
Spustit inicializátor kanálu	hlq.START.CHINIT	CONTROL	Žádná kontrola	-
Spustit modul listener kanálu	hlq.START.LISTENER	CONTROL	Žádná kontrola	-
Spustit připojení SMDS	hlq.START.SMDSCONN	CONTROL	Žádná kontrola	-
Ukončit kanál	hlq.STOP.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Ukončit inicializátor kanálu	hlq.STOP.CHINIT	CONTROL	Žádná kontrola	-
Zastavit modul listener kanálu	hlq.STOP.LISTENER	CONTROL	Žádná kontrola	-
Zastavit připojení SMDS	hlq.STOP.SMDSCONN	CONTROL	Žádná kontrola	-
Pozastavit správce front	hlq.SUSPEND.QMGR	CONTROL	Žádná kontrola	-
Pozastavit klastr správců front	hlq.SUSPEND.QMGR	CONTROL	Žádná kontrola	-

Notes:

1. Prostředek **hlq.TOPIC.topic** se odkazuje na objekt Topic odvozený z TOPCSTR. Další informace viz “Zabezpečení publikování/odběru” na stránce 473

Podrobnosti o profilech PCF produktu IBM MQ , které používají produkt IBM MQ Console, naleznete v příručce “IBM MQ Console -požadované profily zabezpečení příkazu” na stránce 224 .

z/OS *IBM MQ Console -požadované profily zabezpečení příkazu*

Operace prováděné uživatelem v produktu IBM MQ Console uživatelem `MQWebAdmin`nebo `MQWebAdminRO`se provádí v kontextu zabezpečení ID uživatele spuštěných úloh mqweb serveru. Chcete-li použít produkt IBM MQ Console, ID uživatele spuštěné úlohy serveru mqweb potřebuje autorizaci k vydávání určitých příkazů PCF.

Tabulka 51 na stránce 224 zobrazuje pro každý příkaz IBM MQ PCF požadované profily zabezpečení příkazu a odpovídající úroveň přístupu pro každý profil ve třídě MQCMDS, které je zapotřebí 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 prostředků příkazů 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	Žádná kontrola	-
Změnit téma	hlq.ALTER.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
Vymazat frontu	hlq.CLEAR.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER

Tabulka 51. IBM MQ Console příkazy PCF, profily a jejich úrovně přístupu (pokračování)

Příkaz	Profil příkazu pro MQCMDS	Úroveň přístupu pro MQCMDS	Profil prostředků příkazů pro MQADMIN nebo MXADMIN	Úroveň přístupu pro MQADMIN nebo MXADMIN
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	Žádná kontrola	-
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	Žádná kontrola	-
Odstranit téma	hlq.DELETE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
Zjistit objekt ověřovacích informací	hlq.DISPLAY.AUTHINFO	READ (čtení)	Žádná kontrola	-
Zjišťovat názvy objektů ověřovacích informací	hlq.DISPLAY.AUTHINFO	READ (čtení)	Žádná kontrola	-
Zjistit kanál	hlq.DISPLAY.CHANNEL	READ (čtení)	Žádná kontrola	-
Zjistit záznam ověření kanálu	hlq.DISPLAY.CHLAUTH	READ (čtení)	Žádná kontrola	-
Zjistit inicializátor kanálu	hlq.DISPLAY.CHINIT	READ (čtení)	Žádná kontrola	-
Zjistit názvy kanálů	hlq.DISPLAY.CHANNEL	READ (čtení)	Žádná kontrola	-
Zjistit stav kanálu	hlq.DISPLAY.CHSTATUS	READ (čtení)	Žádná kontrola	-
Zjistit frontu	hlq.DISPLAY.QUEUE	READ (čtení)	Žádná kontrola	-
Zjistit správce front	hlq.DISPLAY.QMGR	READ (čtení)	Žádná kontrola	-
Zjistit názvy front	hlq.DISPLAY.QUEUE	READ (čtení)	Žádná kontrola	-
Zjistit stav fronty	hlq.DISPLAY.QSTATUS	READ (čtení)	Žádná kontrola	-
Zjistit odběr	hlq.INQUIRE.SUB	READ (čtení)	Žádná kontrola	-
Zjistit stav odběru	hlq.INQUIRE.SBSTATUS	READ (čtení)	Žádná kontrola	-
Zjistit téma	hlq.DISPLAY.TOPIC	READ (čtení)	Žádná kontrola	-
Zjistit názvy témat	hlq.DISPLAY.TOPIC	READ (čtení)	Žádná kontrola	-
Zjistit stav tématu	hlq.DISPLAY.TPSTATUS	READ (čtení)	Žádná kontrola	-
Odeslat signál Ping pro kanál	hlq.PING.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Aktualizovat klastr	hlq.REFRESH.CLUSTER	ALTER	Žádná kontrola	-
Aktualizovat zabezpečení	hlq.REFRESH.SECURITY	ALTER	Žádná kontrola	-
Resetovat kanál	hlq.RESET.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Vyřešit kanál	hlq.RESOLVE.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL

Tabulka 51. IBM MQ Console příkazy PCF, profily a jejich úrovně přístupu (pokračování)				
Příkaz	**Profil příkazu pro MQCMDS**	**Úroveň přístupu pro MQCMDS**	**Profil prostředků příkazů pro MQADMIN nebo MXADMIN**	**Úroveň přístupu pro MQADMIN nebo MXADMIN**
Nastavit záznam ověření kanálu	hlq.SET.CHLAUTH	CONTROL	Žádná kontrola	-
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 příkazů*

Pokud jste nedefinovali profil přepínače zabezpečení prostředků příkazu, protože chcete kontrolu zabezpečení pro prostředky přidružené k příkazům, musíte přidat profily prostředků pro každý prostředek do příslušné třídy. Tytéž profily zabezpečení řídí příkazy MQSC a PCF.

Pokud jste nedefinovali profil přepínače zabezpečení prostředků příkazů, `hlq.NO.CMD.RESC.CHECKS`, protože chcete kontrolu zabezpečení pro prostředky přidružené k příkazům, musíte:

- Přidejte profil prostředku ve třídě **MQADMIN** , pokud používáte velké profily, pro každý prostředek.
- Přidejte profil prostředku ve třídě **MXADMIN** , pokud používáte pro každý prostředek kombinované profily případu.

Tytéž profily zabezpečení řídí příkazy MQSC a PCF.

Profily pro kontrolu zabezpečení prostředků příkazů mají formát:

```
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 u jednotlivých správců front potlačit definováním profilu úrovně správce front pro tento prostředek příkazu v daném správci front.

Je-li váš správce front členem skupiny sdílení front a používáte-li správce front i zabezpečení na úrovni skupiny sdílení front, produkt IBM MQ nejprve zkontroluje profil s předponou názvu správce front. Pokud ji nenajde, hledá profil s předponou název skupiny sdílení front.

Například název profilu produktu RACF pro kontrolu zabezpečení prostředků příkazů ve vztahu k modelové frontě CREDIT.WORTHY v podsystému CSQ1 je:

```
CSQ1.QUEUE.CREDIT.WORTHY
```

Vzhledem k tomu, že profily pro všechny typy příkazových prostředků jsou umístěny ve třídě MQADMIN, je v profilu zapotřebí část "type" profilu pro rozlišení mezi prostředky různých typů, které mají stejný název. Část názvu profilu "type" může být CHANNEL, QUEUE, TOPIC, PROCESS nebo NAMELIST. Uživatel může být například oprávněn definovat hlq.QUEUE.PAYROLL.ONE, ale nemáte autorizaci k definování hlq.PROCESS.PAYROLL.ONE

Je-li typem prostředku fronta a profil je profil 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 v rámci skupiny sdílení front.

z/OS Příkazy MQSC, profily a jejich úrovně přístupu ukazují pro každý příkaz IBM MQ MQSC, profily nezbytné pro kontrolu zabezpečení příkazů a odpovídající úroveň přístupu pro každý profil ve třídě MQCMDS.

z/OS Příkazy PCF, profily a jejich úrovně přístupu zobrazují pro každý příkaz IBM MQ PCF profily nezbytné pro kontrolu zabezpečení příkazů a odpovídající úroveň přístupu pro jednotlivé profily ve třídě MQCMDS.

z/OS *Kontrola zabezpečení prostředků příkazů pro fronty aliasů a vzdálené fronty*
Fronta aliasů a vzdálené fronty poskytují přesměrování do jiné fronty. Další body se použijí, když zvážíte kontrolu zabezpečení pro tyto fronty.

Alias fronty

Pokud definujete alias frontu, jsou kontroly zabezpečení prostředků příkazů prováděny pouze s názvem fronty aliasů, nikoli s názvem cílové fronty, na kterou je alias interpretováno.

Fronty aliasů se mohou interpretovat jak lokální, tak i vzdálené fronty. Nechcete-li uživatelům povolit přístup k určitým lokálním nebo vzdáleným frontám, musíte provést obě tyto akce:

1. Neumožněte uživatelům přístup k těmto lokálním a vzdáleným frontám.
2. Omezte uživatele tak, aby mohli definovat aliasy pro tyto fronty. To znamená, že zabráníte tomu, aby mohli vydávat příkazy DEFINE QALIAS a ALTER QALIAS.

Vzdálené fronty

Když definujete vzdálenou frontu, jsou kontroly zabezpečení prostředků prováděny pouze proti názvu vzdálené fronty. Žádné kontroly se neprovádí proti názvům 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 k řízení počtu ID uživatelů kontrolovaných pro zabezpečení na úrovni rozhraní API. Tento profil se nazývá profil RESLEVEL. Způsob, jakým tento profil ovlivňuje zabezpečení na úrovni rozhraní API, závisí na tom, jak přistupujete k produktu IBM MQ.

Pokud se aplikace pokusí o připojení k produktu IBM MQ, produkt IBM MQ zkontroluje přístup, který má jméno uživatele přidružené k tomuto 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 uživatele přidružená k jednotlivým typům připojení jsou:

- ID uživatele připojované úlohy pro dávkové připojení
- ID uživatele adresního prostoru CICS pro připojení CICS
- ID uživatele adresního prostoru IMS pro připojení IMS
- ID uživatele adresního prostoru iniciátoru kanálu pro připojení inicializátoru kanálu

Upozornění: RESLEVEL je velmi výkonná volba; může způsobit vynechání všech kontrol zabezpečení prostředků pro určité připojení.

Pokud nemáte definován profil RESLEVEL, musíte být opatrní, aby se žádný jiný profil ve třídě MQADMIN neshoduje s hlq.RESLEVEL. Máte-li například profil v MQADMIN s názvem hlq. * *, a žádný profil hlq.RESLEVEL , pozor na důsledky úlohy hlq. * * profil, protože se používá pro kontrolu RESLEVEL.

Definujte profil hlq.RESLEVEL a nastavte hodnotu UACC na hodnotu NONE, místo abyste žádný profil RESLEVEL vůbec nevytvořili. Je třeba mít 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 252.

Používáte-li pouze zabezpečení na úrovni správce front, produkt IBM MQ provádí kontroly RESLEVEL pro profil produktu `qmgr-name.RESLEVEL` . Používáte-li pouze zabezpečení na úrovni skupiny sdílení front, produkt IBM MQ provádí kontroly RESLEVEL pro profil produktu `qsg-name.RESLEVEL` . Používáte-li kombinaci správce front i zabezpečení na úrovni skupiny sdílení front, produkt IBM MQ nejprve zkontroluje existenci profilu RESLEVEL na úrovni správce front. Pokud ji nenajde, zkontroluje profil RESLEVEL na úrovni skupiny sdílení front.

Pokud nelze najít profil RESLEVEL, IBM MQ povoluje kontrolu úlohy a úlohy (nebo alternativního uživatele) pro připojení CICS nebo IMS . Pro dávkové připojení IBM MQ povoluje kontrolu ID uživatele úlohy (nebo alternativního) uživatele. Pro inicializátor kanálu umožňuje IBM MQ kontrolu ID uživatele kanálu a ID uživatele MCA (nebo alternativního).

Existuje-li profil RESLEVEL, úroveň kontroly závisí na úrovni prostředí a přístupu k profilu.

Pamatujte, že pokud je váš správce front členem skupiny sdílení front a nedefinujete tento profil na úrovni správce front, může existovat jedna definice na úrovni skupiny sdílení front, která bude mít vliv na úroveň checking.To aktivovat kontrolu dvou ID uživatelů, definujete profil RESLEVEL (s předponou s názvem správce front názvu skupiny sdílení front) s UACC (NONE) a ujistěte se, že příslušní uživatelé nemají přístup k tomuto profilu.

Když uvážíte přístup, který má ID uživatele iniciátoru kanálu k parametru RESLEVEL, nezapomeňte, že připojení ustanovené inicializačním programem kanálu je také připojení využívaneným kanály. Nastavení, které způsobí vynechání všech kontrol zabezpečení prostředků pro ID uživatele iniciátoru kanálu efektivně obchází bezpečnostní kontroly pro všechny kanály. Je-li ID uživatele iniciátoru kanálu přístup k souboru RESLEVEL jiným než NONE, je pro přístup kontrolován pouze jedno ID uživatele (pro úroveň přístupu READ nebo UPDATE) nebo žádná ID uživatele (pro úroveň přístupu CONTROL nebo ALTER). Pokud přidělíte ID uživatele iniciátoru kanálu jinou úroveň přístupu než NONE, ujistěte se, že chápete vliv tohoto nastavení na kontroly zabezpečení prováděné pro kanály.

Použití profilu RESLEVEL znamená, že se neprovedou běžné záznamy auditu zabezpečení. Zadáte-li například UAUDIT na uživatele, přístup k profilu hlq.RESLEVEL v MQADMIN se nebude monitorovat.

Pokud použijete volbu WARNING produktu RACF v profilu hlq.RESLEVEL , nebudou pro profily ve třídě RESLEVEL vytvářeny žádné varovné zprávy produktu RACF .

Kontrola zabezpečení pro zprávy sestav, jako např. COD, je řízena profilem RESLEVEL přidruženým k původní aplikaci. Má-li například ID uživatele dávkové úlohy oprávnění CONTROL nebo ALTER pro profil RESLEVEL, bude vynechána kontrola všech prostředků provedených dávkovou úlohou, včetně kontroly zabezpečení zpráv sestav.

Změníte-li profil RESLEVEL, uživatelé se musí před změnou připojení znovu odpojit a znovu připojit. (To zahrnuje zastavení a restart inicializátoru kanálu, pokud je změněn přístup k ID uživatele distribuovaného adresního prostoru fronty do profilu RESLEVEL.)

Chcete-li vypnout auditování RESLEVEL, použijte parametr systému RESAUDIT.

z/OS *RESLEVEL a dávková spojení*

Ve výchozím nastavení platí, že je-li k prostředku IBM MQ přistupován prostřednictvím dávkových a dávkových připojení, musí mít uživatel oprávnění k přístupu k danému prostředku pro konkrétní operaci. Kontrolováním zabezpečení můžete obejít kontrolu zabezpečení nastavením příslušné definice RESLEVEL.

Určuje, zda je uživatel kontrolován nebo není založen na ID uživatele použitém v době připojení, stejné ID uživatele použité pro kontrolu připojení.

Můžete například nastavit RESLEVEL tak, že když uživatel, kterému důvěřujete, přistupuje k určitým prostředkům prostřednictvím dávkového připojení, nejsou provedeny žádné kontroly zabezpečení prostředků API; ale když se uživatel, kterému nedůvěřuje, pokusí o přístup ke stejným prostředkům, kontroly zabezpečení se provedou jako normální. Kontrola RESLEVEL by měla být nastavena pouze tehdy, když jste dostatečně důvěřovali uživateli a programům, které spustil tento uživatel.

Následující tabulka zobrazuje kontroly provedené u dávkových připojení.

Tabulka 52. Kontroly provedené na různých úrovních přístupu RACF pro dávkové připojení	
RACF úroveň přístupu	**Stupeň kontroly**
ŽÁDNÉ	Provedená kontrola prostředků
READ (čtení)	Provedená kontrola prostředků
AKTUALIZOVAT	Provedená kontrola prostředků
CONTROL	Žádná kontrola.
ALTER	Žádná kontrola.

z/OS *RESLEVEL a systémové funkce*

Aplikace RESLEVEL pro operační a ovládací panely a pro CSQUTIL.

Ovládací panely a řídicí panely a obslužný program CSQUTIL jsou aplikace typu dávky, které vytvářejí požadavky na příkazový server správce front, a proto se vztahují na pokyny popsané v části "RESLEVEL a dávková spojení" na stránce 228. Můžete použít RESLEVEL k vynechání kontroly zabezpečení pro SYSTEM.COMMAND.INPUT a SYSTEM.COMMAND.REPLY.MODEL front, 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 přidružena žádná kontrola připojení nebo RESLEVEL. Chcete-li zachovat zabezpečení, musí proto příkazový server potvrdit, že ID uživatele žádající aplikace má oprávnění k otevření fronty používané pro odpovědi. Pro operace a ovládací panely je to SYSTEM.CSQOREXX. *. Pro CSQUTIL je to SYSTEM.CSQUTIL. *. Uživatelé musí mít oprávnění k používání těchto front, jak je popsáno v části "Zabezpečení systémové fronty" na stránce 200, a navíc k libovolné autorizaci RESLEVEL, která jsou jim udělena.

Pro ostatní aplikace používající příkazový server je to fronta, kterou pojmenujete jako jejich odpověď na frontu. Takové jiné aplikace mohou klamat příkazový server na umisťování zpráv do neautorizovaných front předáním (v kontextu zprávy) spolehlivějšího ID uživatele, než je jeho vlastní pro příkazový server. Chcete-li tomu zabránit, použijte profil CONTEXT k ochraně kontextu identity zpráv umístěných v systému SYSTEM.COMMAND.INPUT.

z/OS *Připojení RESLEVEL a CICS*

Je-li při připojení k produktu CICS prováděna kontrola zabezpečení prostředků rozhraní API, je ve výchozím stavu zaškrtnuto dva ID uživatelů. Pomocí nastavení profilu RESLEVEL můžete změnit, která ID uživatele se kontrolují.

První ID uživatele bylo zkontrolováno, že je adresní prostor CICS . Jedná se o ID uživatele na zakázkový list úlohy CICS nebo ID uživatele přiřazeného ke spuštěné úloze CICS podle třídy z/OS STARTED nebo v tabulce 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, který spouští transakci produktu CICS , musí mít přístup k prostředku na správné úrovni.

Jak RESLEVEL může ovlivnit provedené kontroly

V závislosti na tom, jak nastavíte profil RESLEVEL, můžete změnit, která ID uživatelů se kontrolují při požadavku na přístup k prostředku. Další informace viz Tabulka 53 na stránce 230.

Kontrolovaná ID uživatelů závisí na ID uživatele použitém při připojení, to znamená, ID uživatele adresního prostoru CICS . Tento ovládací prvek vám umožňuje obejít kontrolu zabezpečení prostředků API pro požadavky IBM MQ přicházející z jednoho systému (například testovací systém, TESTCICS,), ale implementovat je pro jiný (například produkční systém, PRODCICS).

Poznámka: Pokud jste nastavili ID uživatele adresního prostoru produktu CICS s atributem "trusted" ve třídě STARTED nebo v tabulce spuštěných procedur RACF ICHRIN03, potlačí všechny kontroly ID

uživatele adresního prostoru CICS vytvořeného profilem RESLEVEL pro vašeho správce front (to znamená, že správce front neprovádí kontrolu zabezpečení pro adresní prostor CICS). Další informace naleznete v příručce *CICS Transaction Server for z/OS V3.2 RACF Security Guide*.

V následující tabulce jsou uvedeny kontroly provedené u připojení produktu CICS .

Tabulka 53. Kontroly provedené na různých úrovních přístupu RACF pro připojení CICS

RACF úroveň přístupu	**Stupeň kontroly**
ŽÁDNÉ	Produkt IBM MQ zkontroluje ID uživatele adresního prostoru CICS a ID uživatele transakce.
READ (čtení)	IBM MQ kontroluje pouze ID uživatele adresního prostoru CICS .
AKTUALIZOVAT	Je-li transakce definována na CICS s parametrem RESSEC (YES), produkt IBM MQ zkontroluje ID uživatele adresního prostoru CICS a ID uživatele transakce.
AKTUALIZOVAT	Je-li transakce definována na CICS s RESESEC (NO), IBM MQ kontroluje pouze ID uživatele adresního prostoru CICS .
CONTROL nebo ALTER	Produkt IBM MQ nekontroluje žádná ID uživatelů.

z/OS *Připojení RESLEVEL a IMS*

Je-li pro připojení produktu IMS provedena kontrola zabezpečení prostředků rozhraní API, je při výchozím nastavení zaškrtnuto dvě ID uživatelů. Pomocí nastavení profilu RESLEVEL můžete změnit, která ID uživatele se kontrolují.

Je-li pro připojení produktu IMS provedena kontrola zabezpečení prostředků rozhraní API, je při výchozím nastavení ověřeno, zda je přístup k prostředku povolen, jsou zkontrolována dvě ID uživatelů.

První zaškrtnuté ID uživatele je adresní prostor oblasti IMS . To je převzato buď z pole USER z zakázkového listu, nebo z ID uživatele přiřazeného 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. Je určen podle typu závislé oblasti, jak ukazuje Jak je určeno druhé ID uživatele určené pro připojení produktu IMS(tm).

Pokud buď první, nebo druhé ID uživatele produktu IMS nemá přístup k prostředku, požadavek selže s kódem dokončení MQRC_NOT_AUTHORIZED.

The setting of IBM MQ RESLEVEL profiles cannot alter the user ID under which IMS transactions are scheduled from the IBM-supplied MQ-IMS trigger monitor program CSQQTRMN. Toto ID uživatele je PSBNAME monitoru spouštěčů, což je standardně CSQQTRMN.

Jak RESLEVEL může ovlivnit provedené kontroly

V závislosti na tom, jak nastavíte profil RESLEVEL, můžete změnit, která ID uživatelů se kontrolují při požadavku na 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 .
- Nekontrolovat žádná ID uživatelů.

V následující tabulce jsou uvedeny kontroly provedené u připojení produktu IMS .

Tabulka 54. Kontroly provedené na různých úrovních přístupu RACF pro připojení IMS

RACF úroveň přístupu	**Stupeň kontroly**
ŽÁDNÉ	Zkontrolujte ID uživatele adresního prostoru IMS a ID uživatele druhého uživatele IMS nebo alternativní ID uživatele.

Tabulka 54. Kontroly provedené na různých úrovních přístupu RACF pro připojení IMS (pokračování)	
RACF úroveň přístupu	**Stupeň kontroly**
READ (čtení)	Zkontrolujte ID uživatele adresního prostoru IMS .
AKTUALIZOVAT	Zkontrolujte ID uživatele adresního prostoru IMS .
CONTROL	Žádná kontrola.
ALTER	Žádná kontrola.

z/OS *RESLEVEL a připojení inicializátoru kanálu*

Je-li při kontrole zabezpečení pomocí rozhraní API kanálu provedena kontrola zabezpečení prostředku rozhraní API, jsou zaškrtnutá dvě ID uživatelů. Pomocí nastavení profilu RESLEVEL můžete změnit, která ID uživatele se kontrolují.

Je-li při kontrole zabezpečení pomocí rozhraní API kanálu provedena kontrola zabezpečení prostředku rozhraní API, kontrolují se standardně dvě ID uživatelů, aby bylo možné zjistit, zda je přístup k prostředku povolen.

Kontrolují se ID uživatele, která jsou uvedena atributem kanálu MCAUSER, který byl přijat ze sítě, z adresního prostoru inicializátoru kanálu nebo alternativního ID uživatele pro deskriptor zprávy. Která ID uživatelů jsou kontrolována, závisí na komunikačním protokolu, který používáte, a na nastavení atributu PUTAUT kanálu. Další informace viz “ID uživatele použitá inicializátorem kanálu” na stránce 236.

Pokud jedno z těchto ID uživatelů nemá přístup k prostředku, požadavek selže s kódem dokončení MQRC_NOT_AUTHORIZED.

Jak RESLEVEL může ovlivnit provedené kontroly

V závislosti na tom, jak nastavíte profil RESLEVEL, můžete změnit, která ID uživatelů se kontrolují při požadavku na přístup k prostředku a kolik jich je zkontrolováno.

Následující tabulka zobrazuje kontroly provedené pro připojení inicializátoru kanálu a pro všechny kanály od té doby, co používají toto připojení.

Tabulka 55. Kontroly provedené na různých úrovních přístupu RACF pro připojení inicializátoru kanálu	
RACF úroveň přístupu	**Stupeň kontroly**
ŽÁDNÉ	Zkontrolujte dvě ID uživatelů.
READ (čtení)	Zkontrolujte jedno ID uživatele.
AKTUALIZOVAT	Zkontrolujte jedno ID uživatele.
CONTROL	Žádná kontrola.
ALTER	Žádná kontrola.
Poznámka: Definice kontrolovaných ID uživatelů viz “ID uživatele použitá inicializátorem kanálu” na stránce 236 .	

z/OS *RESLEVEL a řazení do front v rámci skupiny*

Je-li správcem front v rámci skupiny provedena kontrola zabezpečení prostředků rozhraní API, je při výchozím nastavení zkontrolováno, zda je přístup k prostředku povolen, a to pomocí dvou ID uživatelů. Pomocí nastavení profilu RESLEVEL můžete změnit, která ID uživatelů se budou kontrolovat.

Ověkontrolovanou ID uživatelů může být ID uživatele určené atributem IGQUSER přijímajícího správce front, ID uživatele správce front v rámci skupiny sdílení front, který zprávu vložil do systému SYSTEM.QSG.TRANSMIT.QUEUE, nebo alternativní ID uživatele zadané v poli *UserIdentifier*

deskriptoru zpráv zprávy. Další informace viz “ID uživatelů použitá agentem front v rámci skupiny” na stránce 240.

Vzhledem k tomu, že agent fronty v rámci skupiny je interní úloha správce front, nevydá explicitní žádost o připojení a pracuje pod ID uživatele správce front. Agent front intra-group se spustí při inicializaci správce front. Během inicializace agenta řazení do front v rámci skupiny produkt IBM MQ kontroluje přístup, který má ID uživatele přidružený ke správci front k profilu ve třídě MQADMIN s názvem:

```
hlq.RESLEVEL
```

Tato kontrola se provádí vždy, pokud nebyl nastaven přepínač hlq.NO.SUBSYS.SECURITY .

Pokud neexistuje žádný profil RESLEVEL, IBM MQ povolí kontrolu pro dvě ID uživatelů. Existuje-li profil RESLEVEL, úroveň kontroly závisí na úrovni přístupu uděleného ID uživatele správce front pro daný profil. Kontroly provedené při různých úrovních přístupu produktu RACF(r) pro správce front v rámci skupiny zobrazují kontroly provedené u agenta řazení do front v rámci skupiny.

Tabulka 56. Kontroly provedené na různých úrovních přístupu produktu RACF pro agenta intra-group queuing Agent

RACF úroveň přístupu	**Stupeň kontroly**
ŽÁDNÉ	Zkontrolujte dvě ID uživatelů.
READ (čtení)	Zkontrolujte jedno ID uživatele.
AKTUALIZOVAT	Zkontrolujte jedno ID uživatele.
CONTROL	Žádná kontrola.
ALTER	Žádná kontrola.
Poznámka: Definice kontrolovaných ID uživatelů viz “ID uživatelů použitá agentem front v rámci skupiny” na stránce 240 .	

Změní-li se oprávnění udělená profilu RESLEVEL pro ID uživatele správce front, musí být agent fronty v rámci skupiny zastaven a restartován, aby bylo možné nová oprávnění vybrat. Protože neexistuje žádný způsob, jak nezávisle zastavit a restartovat agenta intra-group queuing, musí být správce front zastaven a restartován, aby toho bylo možné dosáhnout.

z/OS *RESLEVEL a ID uživatelů zkontrolováno*

Příklad nastavení profilu RESLEVEL a udělení přístupu k němu.

Kontrola ID uživatele vzhledem k názvu profilu pro dávkové připojení prostřednictvím volby ID uživatele zkontrolovaná proti názvu profilu pro LU 6.2 a kanály připojení serveru TCP/IP ukazují, jak RESLEVEL ovlivňuje, která ID uživatelů jsou kontrolována pro různé požadavky MQI.

Předpokládejme například, že máte správce front s názvem QM66 s následujícími požadavky:

- Uživatel WS21B má být vynechán ze zabezpečení prostředků.
- CICS spuštěná úloha WXNCICS spuštěná pod ID uživatele adresního prostoru CICSWXN má provést úplnou kontrolu prostředků pouze pro transakce definované s ESPREC (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 během připojení uživatelských jmen ke správci front QM66, uživatelé se musí před změnou připojení znovu odpojit a znovu připojit.

Není-li zabezpečení subsystému aktivní, když se uživatel připojuje, ale když je tento uživatel stále připojen, stane se zabezpečení podsystému aktivní, kontrola zabezpečení celého prostředku se použije na uživatele. Aby bylo možné získat správné zpracování RESLEVEL, musí se uživatel znovu připojit.

z/OS ID uživatelů pro kontrolu zabezpečení v systému z/OS

Produkt IBM MQ spouští kontroly zabezpečení založené na 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 uživatele pro zabezpečení připojení*

ID uživatele použité pro zabezpečení připojení závisí na typu připojení.

Typ připojení	Obsah ID uživatele
Dávkové připojení	ID uživatele připojované úlohy. Příklad: • ID uživatele TSO • ID uživatele přiřazené dávkové úloze pomocí parametru USER JCL • ID uživatele přiřazeného ke spuštěné úloze podle třídy STARTED nebo tabulky spuštěných procedur
CICS připojení	ID uživatele adresního prostoru CICS .
IMS připojení	ID uživatele adresního prostoru oblasti IMS .
Připojení inicializátoru kanálu	ID uživatele adresního prostoru iniciátoru kanálu.

z/OS *ID uživatele pro zabezpečení příkazů a zabezpečení prostředků*

ID uživatele použité pro zabezpečení příkazů nebo zabezpečení prostředků příkazů závisí na tom, odkud je příkaz vydán.

Vydáno z ...	Obsah ID uživatele
CSQINP1, CSQINP2, nebo CSQINPT	Neprovede se žádná kontrola.
Vstupní fronta systémového příkazu	ID uživatele nalezeného v *UserIdentifier* deskriptoru zprávy, který obsahuje příkaz. Pokud zpráva neobsahuje *UserIdentifier*, předá se správci zabezpečení ID uživatele mezery.
Konzola	ID uživatele přihlášené na konzolu. Není-li konzola přihlášena, výchozí ID uživatele nastavené systémovým parametrem CMDUSER v souboru CSQ6SYSP. Chcete-li vydávat příkazy z konzoly, musí mít konzola atribut z/OS SYS AUTHORITY.
Konzola SDSF/TSO	TSO nebo ID uživatele úlohy.
Ovládací panely a ovládací panely	ID uživatele TSO. Chcete-li používat operace a ovládací panely, musíte mít příslušné oprávnění k vydávání příkazů odpovídajících vámi vybízným akcím. Kromě toho musíte mít přístup pro čtení ke všem položkám hlq.DISPLAY. Profily *objektu* ve třídě MQCMDS, protože panely používají různé příkazy DISPLAY ke shromažďování informací, které mají k dispozici.

Vydáno z ...	Obsah ID uživatele
MGCRE	Je-li MGCRE použito s UTOKEN, ID uživatele v UTOKEN. Je-li MGCRE vydán bez použití UTOKEN, použije se TSO nebo ID uživatele úlohy.
CSQ0UTIL	ID uživatele úlohy.
KALKUNIT	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 běžné a alternativní ID uživatele pro každý typ připojení. Počet kontrol je definován profilem RESLEVEL. ID uživatele, které bylo zkontrolováno, je použito pro volání **MQOPEN**, **MQSUB**nebo **MQPUT1** .

Poznámka: Všechna pole ID uživatele se kontrolují přesně tak, jak jsou přijata. Nejsou provedeny žádné konverze, a například tři pole s ID uživatele obsahující "Bob", "BOB"a "bob" nejsou ekvivalentní.

z/OS *ID uživatele byla zkontrolována pro připojení dávky*

ID uživatele kontrolované pro dávkové připojení závisí na tom, jak je úloha spuštěna a zda bylo zadáno alternativní ID uživatele.

Tabulka 57. Kontrola ID uživatele vzhledem k názvu profilu pro dávkové připojení

Alternativní ID uživatele zadané při otevření?	hlq.ALTERNATE.USER.userid	Profil hlq.CONTEXT.queuename	Profil hlq.resourcename
Ne	-	Úloha	Úloha
Ano	Úloha	Úloha	KLÁVESA ALT

Klíč:

KLÁVESA ALT
Alternativní ID uživatele.

Úloha

- ID uživatele přihlášení TSO nebo z/OS UNIX System Services .
- ID uživatele přiřazené dávkové úloze.
- ID uživatele přiřazeného ke spuštěné úloze podle třídy STARTED nebo tabulky spuštěných procedur.
- ID uživatele přidružené k provádění uložené procedury Db2

Dávková úloha provádí operaci MQPUT1 do fronty s názvem Q1 s hodnotou RESLEVEL nastavenou na hodnotu READ a alternativní kontrola ID uživatele byla vypnuta.

Kontroly provedené na různých úrovních přístupu RACF(r) pro dávkové připojení a Kontrola ID uživatele vzhledem k názvu profilu pro dávkové připojení ukazují, že ID uživatele úlohy je zkontrolováno proti profilu hlq.Q1.

z/OS *ID uživatelů zkontrolována pro připojení CICS*

ID uživatelů kontrolovaná pro připojení CICS závisí na tom, zda má být provedena jedna nebo dvě kontroly a zda je zadáno alternativní ID uživatele.

Tabulka 58. Kontrola ID uživatele pro jméno profilu pro CICS-type ID uživatele			
Alternativní ID uživatele zadané při otevření?	**hlq.ALTERNATE.USER.userid**	**Profil hlq.CONTEXT.queuename**	**Profil hlq.resourcename**
Ne, 1 kontrola	-	PÍ	PÍ
Ne, 2 kontroly	-	ADS + TXN	ADS + TXN
Ano, 1 kontrola	PÍ	PÍ	PÍ
Ano, 2 kontroly	ADS + TXN	ADS + TXN	ADS + ALT

Klíč:

KLÁVESA ALT
Jméno alternativního uživatele

PÍ
ID uživatele přidružené k dávkové úloze CICS nebo, pokud je CICS spuštěn jako spuštěná úloha, přes třídu STARTED nebo tabulku 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 uživatele, která se kontrolují za následujících podmínek:

- Úroveň přístupu RACF k profilu RESLEVEL, pro ID uživatele adresního prostoru CICS je nastavena na hodnotu NONE.
- Volání MQOPEN je vytvořeno pro frontu s MQOO_OUTPUT a MQOO_PASS_IDENTITY_CONTEXT.

Nejprve si prohlédněte, kolik ID uživatelů produktu CICS je kontrolováno na základě ID uživatele CICS adresního prostoru uživatele k přístupu k profilu RESLEVEL. V produktu Tabulka 53 na stránce 230 v tématu “Připojení RESLEVEL a CICS” na stránce 229jsou zkontrolována dvě ID uživatelů, je-li profil RESLEVEL nastaven na hodnotu NONE. Pak od Tabulka 58 na stránce 235 jsou tyto kontroly prováděny:

- Příkaz hlq.ALTERNATE.USER.userid není kontrolován.
- Profil hlq.CONTEXT.queuename je kontrolován s ID uživatele adresního prostoru CICS i ID uživatele transakce CICS .
- Profil hlq.resourcename je zkontrolován jak s ID uživatele adresního prostoru CICS , tak i s ID uživatele transakce CICS .

To znamená, že jsou provedeny čtyři kontroly zabezpečení pro toto volání MQOPEN .

z/OS *ID uživatelů zkontrolována pro připojení IMS*

ID uživatelů kontrolovaná pro připojení produktu IMS závisí na tom, zda má být provedena jedna nebo dvě kontroly a zda je určeno alternativní ID uživatele. Je-li zaškrtnuté druhé ID uživatele, závisí na typu závislé oblasti a na tom, která ID uživatele jsou k dispozici.

Tabulka 59. Kontrola ID uživatele pro jméno profilu pro IMS-type ID uživatele			
Alternativní ID uživatele zadané při otevření?	**hlq.ALTERNATE.USER.userid**	**Profil hlq.CONTEXT.queuenam e**	**Profil hlq.resourcename**
Ne, 1 kontrola	-	REG.	REG.
Ne, 2 kontroly	-	REG + SEC	REG + SEC
Ano, 1 kontrola	REG.	REG.	REG.
Ano, 2 kontroly	REG + SEC	REG + SEC	REG. NEBO

Klíč:

KLÁVESA ALT
Alternativní ID uživatele.

REG.
ID uživatele je obvykle nastaveno prostřednictvím třídy STARTED nebo v tabulce spuštěných procedur nebo, pokud je IMS spuštěný, z odeslané úlohy parametrem USER JCL.

Sek
Druhé ID uživatele je přidruženo k práci, která se provádí v závislé oblasti. Je určen podle Tabulka 60 na stránce 236.

Tabulka 60. Jak je určeno druhé ID uživatele pro připojení produktu IMS

Typy závislých oblastí	Hierarchie pro určení druhého ID uživatele
• Byla vydána zpráva BMP a bylo vydáno úspěšné GET UNIQUE. • IFP a GET UNIQUE vydané. • MPP.	ID uživatele přidružené k transakci IMS , pokud je uživatel přihlášen. Název LTERM, pokud je dostupný. PSBNAME.
• Zpráva BMP vyvolaná a úspěšná metoda GET UNIQUE nebyla vydána. • BMP neřízená zprávou. • IFP a GET UNIQUE nebyly vydány.	ID uživatele přidružené k adresnímu prostoru oblasti závislé na IMS , pokud se nejedná o všechny mezery nebo samé nuly. PSBNAME.

z/OS *ID uživatele použitá inicialiátorem kanálu*
Tato kolekce témat popisuje používaná a zaškrtnutá jména uživatelů pro přijímací kanály a pro klientské požadavky MQI vydané přes kanály připojení serveru. Informace jsou poskytnuty pro TCP/IP a pro LU6.2

K určení typu použité kontroly zabezpečení můžete použít parametr PUTAUT v definici přijímajícího kanálu. Chcete-li zajistit konzistentní kontrolu zabezpečení v rámci celé sítě produktu IBM MQ , můžete použít volby ONLYMCA a ALTMCA.

K určení identifikátoru uživatele použitého agentem MCA můžete použít příkaz DISPLAY CHSTATUS.

z/OS *Příjem kanálů pomocí protokolu TCP/IP*
Kontrolovaná ID uživatelů závisí na volbě PUTAUT kanálu a na tom, zda má být provedena jedna nebo dvě kontroly.

Tabulka 61. ID uživatelů byly zkontrolována proti názvu profilu pro kanály TCP/IP

Volba PUTAUT zadaná v kanálu příjemce nebo žadatele	hlq.ALTERNATE.USER.userid	Profil hlq.CONTEXT.queuename	Profil hlq.resourcename
DEF, 1 kontrola	-	CHL	CHL
DEF, 2 kontroly	-	CHL + MCA	CHL + MCA
Kontrola CTX, 1	CHL	CHL	CHL
CTX, 2 kontroly	CHL + MCA	CHL + MCA	CHL + ALT
ONLYMCA, 1 kontrola	-	MCA	MCA
ONLYMCA, 2 kontroly	-	MCA	MCA

Tabulka 61. ID uživatelů byly zkontrolována proti názvu profilu pro kanály TCP/IP (pokračování)			
Volba PUTAUT zadaná v kanálu příjemce nebo žadatele	**hlq.ALTERNATE.USER.userid**	**Profil hlq.CONTEXT.queuename**	**Profil hlq.resourcename**
ALTMCA, 1 kontrola	MCA	MCA	MCA
ALTMCA, 2 kontroly	MCA	MCA	MCA + ALT

Klíč:

MCA (ID uživatele MCA)
ID uživatele zadané pro atribut kanálu MCAUSER na přijímači; je-li prázdné, použije se ID uživatele adresního prostoru kanálu příjemce na straně příjemce nebo žadatele.

CHL (ID uživatele kanálu)
V TCP/IP není zabezpečení podporováno komunikačním systémem pro kanál. Je-li používáno zabezpečení TLS (Transport Layer Security) a byl od partnera přenášen digitální certifikát, použije se ID uživatele přidružené k tomuto certifikátu (je-li nainstalován) nebo ID uživatele přidružené k odpovídajícímu filtru nalezenému pomocí RACF filtrování názvu certifikátu (CNF). Pokud není nalezeno žádné přidružené ID uživatele, nebo pokud se nepoužívá TLS, použije se ID uživatele adresního prostoru iniciátoru kanálu přijímajícího nebo žadatelského konce jako ID uživatele kanálu na kanálech definovaných s parametrem PUTAUT nastaveným na DEF nebo CTX.

Poznámka: Použití filtrování názvu certifikátu produktu RACF (CNF) vám umožňuje přiřadit stejné ID uživatele produktu RACF k více vzdáleným uživatelům, například všechny uživatele ve stejné organizační jednotce, kteří by přirozeně měli mít stejné oprávnění zabezpečení. To znamená, že server nemusí mít kopii certifikátu každého možného vzdáleného uživatele na celém světě a výrazně zjednodušuje správu a distribuci certifikátů.

Je-li parametr PUTAUT nastaven na hodnotu ONLYMCA nebo ALTMCA pro daný kanál, je ID uživatele kanálu ignorováno a použije se ID uživatele MCA přijímače nebo žadatele. To platí i pro kanály TCP/IP, které používají TLS.

ALT (Alternativní ID uživatele)
ID uživatele z informací o kontextu (to znamená pole *UserIdentifier*) v rámci deskriptoru zprávy. Toto ID uživatele je přesunuto do pole *AlternateUserID* v deskriptoru objektu před zadáním volání **MQOPEN** nebo **MQPUT1** pro cílovou cílovou frontu.

z/OS *Příjem kanálů pomocí LU 6.2*

Kontrolovaná ID uživatelů závisí na volbě PUTAUT kanálu a na tom, zda má být provedena jedna nebo dvě kontroly.

Tabulka 62. ID uživatelů zkontrolována oproti názvu profilu pro kanály LU 6.2			
Volba PUTAUT zadaná v kanálu příjemce nebo žadatele	**hlq.ALTERNATE.USER.userid**	**Profil hlq.CONTEXT.queuename**	**Profil hlq.resourcename**
DEF, 1 kontrola	-	CHL	CHL
DEF, 2 kontroly	-	CHL + MCA	CHL + MCA
Kontrola CTX, 1	CHL	CHL	CHL
CTX, 2 kontroly	CHL + MCA	CHL + MCA	CHL + ALT
ONLYMCA, 1 kontrola	-	MCA	MCA

Tabulka 62. ID uživatelů zkontrolována oproti názvu profilu pro kanály LU 6.2 (pokračování)			
Volba PUTAUT zadaná v kanálu příjemce nebo žadatele	**hlq.ALTERNATE.USER.userid**	**Profil hlq.CONTEXT.queuename**	**Profil hlq.resourcename**
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 zadané pro atribut kanálu MCAUSER na přijímači; je-li prázdné, použije se ID uživatele adresního prostoru kanálu příjemce na straně příjemce nebo žadatele.

CHL (ID uživatele kanálu)

Kanály žadatele-server
Pokud je kanál spuštěn od žadatele, neexistuje žádná příležitost pro přijetí ID uživatele sítě (ID uživatele kanálu).

Je-li parametr PUTAUT nastaven na DEF nebo CTX na žadatelský kanál, ID uživatele kanálu je ID adresního prostoru iniciátoru kanálu žadatele, protože není přijato žádné ID uživatele ze sítě.

Je-li parametr PUTAUT nastaven na hodnotu ONLYMCA nebo ALTMCA, ID uživatele kanálu se ignoruje a použije se ID uživatele MCA pro žadatele.

Další typy kanálů
Je-li parametr PUTAUT nastaven na DEF nebo CTX na přijímači nebo žadatelský kanál, ID uživatele kanálu je ID uživatele přijaté z komunikačního systému, když je kanál iniciován.

- Pokud je odesílací kanál v systému z/OS, přijatý ID uživatele kanálu je ID uživatele adresního prostoru kanálu iniciátoru kanálu odesílatele.
- Je-li odesílající kanál na jiné platformě (například AIX), přijaté ID uživatele kanálu je obvykle poskytováno parametrem USERID definice kanálu.

Pokud je přijaté ID uživatele prázdné, nebo pokud není přijato žádné ID uživatele, použije se ID uživatele kanálu.

ALT (Alternativní ID uživatele)
ID uživatele z informací o kontextu (to znamená pole *UserIdentifier*) v rámci deskriptoru zprávy. Toto ID uživatele je přesunuto do pole *AlternateUserID* v deskriptoru objektu před voláním operace MQOPEN nebo volání MQPUT1 pro cílovou cílovou frontu.

z/OS *Požadavky klienta MQI*

Lze použít různá ID uživatelů, v závislosti na tom, které ID uživatele a proměnné prostředí byly nastaveny. Tato ID uživatelů jsou kontrolována proti různým profilům, v závislosti na použité volbě PUTAUT a na tom, zda je zadáno alternativní ID uživatele.

Tato sekce popisuje ID uživatelů, která byla zkontrolována pro požadavky klienta MQI vydané prostřednictvím kanálů připojení serveru pro protokol TCP/IP a LU 6.2. ID uživatele MCA a ID uživatele kanálu jsou určeny pro kanály TCP/IP a LU 6.2 popsané v předchozích sekcích.

Pro kanály připojení serveru se použije ID uživatele přijaté od klienta, je-li atribut MCAUSER prázdný.

Další informace viz “Řízení přístupu pro klienty” na stránce 96.

Pro požadavky klienta **MQOPEN**, **MQSUB**a **MQPUT1** použijte následující pravidla k určení profilu, který se kontroluje:

- Pokud je v požadavku uvedeno oprávnění alternativního uživatele, provede se kontrola proti příkazu *hlq*.ALTERNATE.USER. Profil *userid* .
- Pokud požadavek specifikuje oprávnění ke kontextu, provede se kontrola proti *hlq*.KONTEXT. Profil *queuename* .
- Pro všechny požadavky **MQOPEN**, **MQSUB**a **MQPUT1** se provádí kontrola na profilu *hlq.resourcename* .

Když jste určili, které profily se kontrolují, použijte následující tabulku k určení, která ID uživatelů jsou kontrolována proti těmto profilům.

Tabulka 63. ID uživatelů byly zkontrolovány proti názvu profilu pro LU 6.2 a kanály připojení k serveru TCP/IP

Volba PUTAUT zadaná v kanálu připojení serveru	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	CHL + MCA
DEF, 2 kontroly	Ano	CHL + MCA	CHL + MCA	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 na serveru-connection; je-li prázdné, použije se ID uživatele adresního prostoru kanálu kanálu.

CHL (ID uživatele kanálu)
V TCP/IP není zabezpečení podporováno komunikačním systémem pro kanál. Je-li používáno zabezpečení TLS (Transport Layer Security) a byl od partnera přenášen digitální certifikát, použije se ID uživatele přidružené k tomuto certifikátu (je-li nainstalován) nebo ID uživatele přidružené k odpovídajícímu filtru nalezenému pomocí RACF filtrování názvu certifikátu (CNF). Pokud není nalezeno žádné přidružené ID uživatele nebo pokud se TLS nepoužívá, použije se ID uživatele adresního prostoru pro iniciátor kanálu jako ID uživatele kanálu na kanálech definovaných s parametrem PUTAUT nastaveným na DEF nebo CTX.

Poznámka: Použití filtrování názvu certifikátu produktu RACF (CNF) vám umožňuje přiřadit stejné ID uživatele produktu RACF k více vzdáleným uživatelům, například všechny uživatele ve stejné organizační jednotce, kteří by přirozeně měli mít stejné oprávnění zabezpečení. To znamená, že server nemusí mít kopii certifikátu každého možného vzdáleného uživatele na celém světě a výrazně zjednodušuje správu a distribuci certifikátů.

Je-li parametr PUTAUT nastaven na hodnotu ONLYMCA nebo ALTMCA pro daný kanál, je ID uživatele kanálu ignorováno a použije se ID uživatele MCA kanálu připojení serveru. To platí i pro kanály TCP/IP, které používají TLS.

ALT (Alternativní ID uživatele)
ID uživatele z informací o kontextu (to znamená pole *UserIdentifier*) v rámci deskriptoru zprávy. Toto ID uživatele se přesune do pole *AlternateUserID* v objektu nebo deskriptoru odběru, dříve než je vydán příkaz **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 přeloží do fronty s názvem QB ve správci front QM02. Zpráva se odešle na kanál TCP/IP s názvem QM01.TO.QM02. Hodnota RESLEVEL je nastavena na hodnotu NONE a operace otevření se provádí s alternativním ID uživatele a kontrolou kontextu. Definice přijímacího kanálu má hodnotu PUTAUT (CTX) a ID uživatele MCA je nastaveno. Která ID uživatele se používají v přijímajícím kanálu k vložení zprávy do fronty QB?

Odpověď: Tabulka 55 na stránce 231 zobrazuje, že jsou zkontrolována dvě ID uživatelů, protože RESLEVEL je nastaven na NONE.

Tabulka 61 na stránce 236 ukazuje, že s parametrem PUTAUT nastaveným na CTX a 2, jsou zkontrolována následující ID uživatelů:

- ID uživatele iniciátoru kanálu a ID uživatele MCAUSER se kontrolují proti příkazu hlq.ALTERNATE.USER.userid .
- ID uživatele iniciátoru kanálu a ID uživatele MCAUSER se kontrolují proti profilu hlq.CONTEXT.queuename .
- ID uživatele iniciátoru kanálu a alternativní ID uživatele uvedené v deskriptoru zpráv (MQMD) se kontrolují proti profilu hlq.Q2 .

z/OS *ID uživatelů použitá agentem front v rámci skupiny*

ID uživatelů, která jsou zkontrolována při otevření cílových front pro správce front v rámci skupiny, jsou určovány hodnotami atributů správce front IGQAUT a IGQUSER.

Možné ID uživatele jsou:

ID uživatele pro řazení do front v rámci skupiny (IGQ)
ID uživatele určené atributem IGQUSER přijímajícího správce front. Je-li tato hodnota nastavena na prázdné místo, použije se ID uživatele přijímajícího správce front. Vzhledem k tomu, že přijímající správce front má oprávnění pro přístup ke všem definovaným frontám, kontroly zabezpečení se u ID uživatele přijímajícího správce front neprovádějí. V tomto případě:

- Pokud má být zkontrolováno pouze jedno ID uživatele a ID uživatele přijímacího správce front, žádné kontroly zabezpečení se neprovedou. To může nastat, když je IGQAUT nastaveno na ONLYIGQ nebo ALTIGQ.
- Pokud mají být zkontrolována dvě ID uživatelů a jedno z ID uživatelů je ID přijímajícího správce front, kontroly zabezpečení se provedou pouze pro jiné ID uživatele. To může nastat, když je IGQAUT nastaveno na DEF, CTX nebo ALTIGQ.
- Pokud mají být zkontrolována dvě ID uživatelů a jsou-li jména uživatelů přijímajícím správcem front, žádné kontroly zabezpečení se neprovedou. To může nastat, když je IGQAUT nastaveno na ONLYIGQ.

Odeslání ID uživatele správce front (SND)
ID uživatele správce front v rámci skupiny sdílení front, do níž byla zpráva umístěna do systému SYSTEM.QSG.TRANSMIT.QUEUE.

Alternativní ID uživatele (ALT)
ID uživatele uvedené v poli *UserIdentifier* v deskriptoru zprávy zprávy.

Tabulka 64. ID uživatelů zkontrolovaná vzhledem k názvu profilu pro řazení do front 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
Kontrola CTX, 1	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:

KLÁVESA ALT
Alternativní ID uživatele.

IGQ
ID uživatele IGQ.

SND
Odesílá se ID uživatele správce front.

z/OS *Prázdné ID uživatele a úrovně UACC*

Pokud dojde k mezerové ID uživatele, je přihlášen RACF nedefinovaný uživatel. Nepřidělte přístup k nedefinovanému uživateli v rozsahu bez omezení.

Prázdné ID uživatele může existovat, když uživatel manipuluje se zprávami pomocí kontextu nebo alternativního zabezpečení uživatele, nebo když IBM MQ projde prázdné ID uživatele. Prázdné ID uživatele se například použije, když je zpráva zapsána do vstupní fronty příkazového systému bez kontextu.

Poznámka: ID uživatele " * " (To znamená, že znak hvězdička následovaný sedmi mezerami) je považován za nedefinované ID uživatele.

Příkaz IBM MQ předá prázdné ID uživatele do produktu RACF a je přihlášen RACF nedefinovaný uživatel. Všechny bezpečnostní kontroly pak použijí univerzální přístup (UACC) pro příslušný profil. V závislosti na tom, jak jste nastavili úrovně přístupu, UACC může dát nedefinovanému uživateli přístup s rozsahem platnosti.

Pokud například vydáte tento příkaz RACF z TSO:

```
RDEFINE MQQUEUE Q.AVAILABLE.TO.EVERYONE UACC(UPDATE)
```

Definujete profil, který umožňuje uživatelem definované ID uživatelů z/OS(která nebyla vložena do seznamu pro přístup) a RACF nedefinované ID uživatele pro vkládání zpráv a získání zpráv od této fronty.

Chcete-li chránit před prázdnými ID uživatelů, musíte pečlivě plánovat úroveň přístupu a omezit počet osob, které mohou používat kontext a zabezpečení alternativního uživatele. Musíte zabránit osobám, které používají nedefinované ID uživatele produktu RACF , přístup k prostředkům, k jejichž přístupu nemají přístup. Zároveň však musíte povolit přístup osobám s definovanými uživatelskými ID. Chcete-li to provést, můžete zadat ID uživatele hvězdička (*) v příkazu RACF PERMIT, který umožňuje přístup k prostředkům pro všechna definovaná ID uživatelů. Proto jsou všechna nedefinovaná ID uživatele (jako

např. " * ") jsou odepřený přístup. Například tyto příkazy RACF zabraňují RACF nedefinovanému ID uživatele získat přístup do fronty k 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 Správa zabezpečení produktu IBM MQ for z/OS

Produkt IBM MQ používá tabulku v paměti k ukládání informací týkajících se jednotlivých uživatelů a žádostí o přístup jednotlivých uživatelů. Chcete-li efektivně spravovat tuto tabulku a snížit počet požadavků z produktu IBM MQ na externího správce zabezpečení (ESM), je k dispozici řada ovládacích prvků.

Tyto ovládací prvky jsou dostupné prostřednictvím jak operací, tak řídicích panelů a příkazů IBM MQ .

z/OS *Přeověřování ID uživatele*

Pokud byla například změněna definice RACF uživatele, který používá prostředky IBM MQ , například připojením uživatele k nové skupině, můžete správci front sdělit, aby tento uživatel znovu podepsal při příštím pokusu o přístup k prostředku IBM MQ . To můžete provést pomocí příkazu IBM MQ RVERIFY SECURITY.

- Uživatel HX0804 získává a umisťuje zprávy do front PAYROLL ve správci front PRD1. Avšak HX0804 nyní vyžaduje přístup k některým frontám PENSION ve stejném správci front (PRD1).
- Administrátor zabezpečení dat připojí uživatele HX0804 do skupiny RACF , která umožňuje přístup k frontám PENSION.
- Takže HX0804 může přistoupit k frontám PENSION okamžitě (tj. bez vypnutí správce front PRD1 nebo čekání na vypršení časového limitu HX0804) musíte použít příkaz IBM MQ :

```
RVERIFY SECURITY(HX0804)
```

Poznámka: Pokud vypnete časový limit ID uživatele po dlouhou dobu (dny nebo týdny), zatímco je správce front spuštěn, musíte si zapamatovat spuštění příkazu RVERIFY SECURITY pro všechny uživatele, kteří byli odvolaní nebo odstraněni v této době.

z/OS *Časové limity ID uživatele*

Po určité době nečinnosti můžete produkt IBM MQ odhlásit od správce front.

Když uživatel přistupuje k prostředku produktu IBM MQ , pokusí se správce front o přihlášení tohoto uživatele do správce front (je-li aktivní zabezpečení subsystému). To znamená, že je uživatel ověřen pro ESM. Tento uživatel zůstane přihlášen k produktu IBM MQ , dokud nebude správce front vypnut, nebo dokud ID uživatele *vypršelo* (ověření se neukončí) nebo se znovu ověří (reověřená).

Když dojde k vypršení časového limitu uživatele, je ID uživatele *odhlášen* ve správci front a všechny informace související s bezpečností uchované pro tohoto uživatele byly zrušeny. Odpisování a odhlášení uživatele v rámci správce front není zjevné pro aplikační program nebo pro uživatele.

Uživatelé jsou způsobilí pro vypršení časového limitu, když nepoužili žádné prostředky IBM MQ pro předem určenou dobu. Toto časové období je nastaveno pomocí příkazu MQSC ALTER SECURITY.

V příkazu ALTER SECURITY lze zadat dvě hodnoty:

VYPRŠENÍ ČASOVÉHO LIMITU
Časové období v minutách, kdy nepoužívané ID uživatele a jeho přidružené prostředky mohou zůstat ve správci front IBM MQ .

INTERVAL
Časové období v minutách mezi kontrolami ID uživatelů a jejich přidružených prostředků, aby bylo možné určit, zda vypršela platnost *TIMEOUT* .

Například, je-li hodnota *TIMEOUT* 30 a hodnota *INTERVAL* je 10, každé 10 minut IBM MQ kontroluje ID uživatelů a jejich přidružené prostředky, aby určil, zda nebyly některé z nich použity po dobu 30 minut. Pokud je nalezeno ID uživatele, jehož časový limit vypršel, je toto ID uživatele odhlášeno v rámci správce front. Dojde-li k nalezení všech informací o vypršení časového limitu přidružených k ID uživatelů bez časového limitu, budou informace o prostředku zrušeny. Pokud nechcete časový limit ID uživatelů používat, nastavte hodnotu parametru *INTERVAL* na nulu. Je-li však hodnota parametru *INTERVAL* nulová, úložiště obsazeno 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 uživatelů bez jednoho uživatele. Nastavíte-li krátký časový interval a hodnoty časového limitu, budou uvolněny prostředky, které již nejsou zapotřebí.

Poznámka: Pokud použijete hodnoty pro *INTERVAL* nebo *TIMEOUT* jiné než výchozí nastavení, musíte znovu zadat příkaz při každém spuštění správce front. To lze provést automaticky vložením 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 do mezipaměti data produktu RACF pro zlepšení výkonu. Když změníte určité třídy zabezpečení, musíte aktualizovat tyto informace uložené v mezipaměti. Nepravidelně obnovujte zabezpečení z výkonnostních důvodů. Můžete se také rozhodnout aktualizovat pouze informace o zabezpečení TLS.

Když je fronta otevřena poprvé (nebo poprvé od obnovení zabezpečení), IBM MQ provede kontrolu RACF za účelem získání přístupových práv uživatele a umístí tyto informace do mezipaměti. Data v mezipaměti zahrnují ID uživatelů a prostředky, na kterých byla provedena kontrola zabezpečení. Je-li fronta znovu otevřena stejným uživatelem, přítomnost dat uložených v mezipaměti znamená, že produkt IBM MQ nemusí vydávat RACF kontroly, což zlepšuje výkonnost. Cílem akce aktualizace zabezpečení je zrušit všechny informace o zabezpečení uložené v mezipaměti a vynutit tak IBM MQ novou kontrolu nad produktem RACF. Kdykoli přidáte, změníte nebo odstraníte profil prostředků produktu RACF , který je zadržen ve třídě MQADMIN, MXADMIN, MQPROC, MXQUEUE, MXQUEUE, MXQUEUE, MQNLIST nebo MXTOPIC, nebo MXTOPIC, musíte sdělit správcům front, kteří používají tuto třídu, aby aktualizovaly informace o zabezpečení, které zadržují. Chcete-li to provést, zadejte následující příkazy:

- Příkaz RACF SETROPTS RACLIST (classname) REFRESH, který se má obnovit na úrovni RACF .
- Příkaz IBM MQ REFRESH SECURITY , který aktualizuje informace o zabezpečení uložené správcem front. Tento příkaz musí vydat každý správce front, který má přístup k profilům, které se změnily. Máte-li skupinu sdílení front, můžete použít atribut oboru příkazu k přímému zadání příkazu pro všechny správce front ve skupině.

  Poznámka: Pokud jste připojili nového uživatele k existující skupině, je třeba spustit příkaz IBM MQ RVERIFY SECURITY(userid). Příkaz REFRESH SECURITY (*) nenechá správce front přihlásit tohoto uživatele znovu, při příštím pokusu o přístup k prostředku IBM MQ .

Používáte-li generické profily v libovolné třídě produktu IBM MQ , musíte při změně, přidání nebo odstranění všech generických profilů zadat také normální příkazy pro aktualizaci produktu RACF . Příklad: SETROPTS GENERIC (název_třídy) OBNOVIT.

Pokud je však profil prostředků RACF přidán, změněn nebo odstraněn a prostředek, ke kterému se vztahuje, nebyl dosud zpřístupněn (proto nejsou do mezipaměti uloženy žádné informace), produkt IBM MQ použije nové informace RACF bez vydání příkazu REFRESH SECURITY.

Je-li zapnuto monitorování RACF , (například pomocí příkazu RACF RALTER AUDIT (access-pokus (audit_access_level)), žádné ukládání do mezipaměti se nekoná, a proto IBM MQ odkazuje přímo na prostor RACF dataspace pro každou kontrolu. Změny jsou proto okamžitě vyzvednuty a REFRESH

SECURITY není nutná pro přístup ke změnám. Můžete potvrdit, zda je monitorování RACF zapnuto, pomocí příkazu RACF RLIST. Můžete například zadat příkaz:

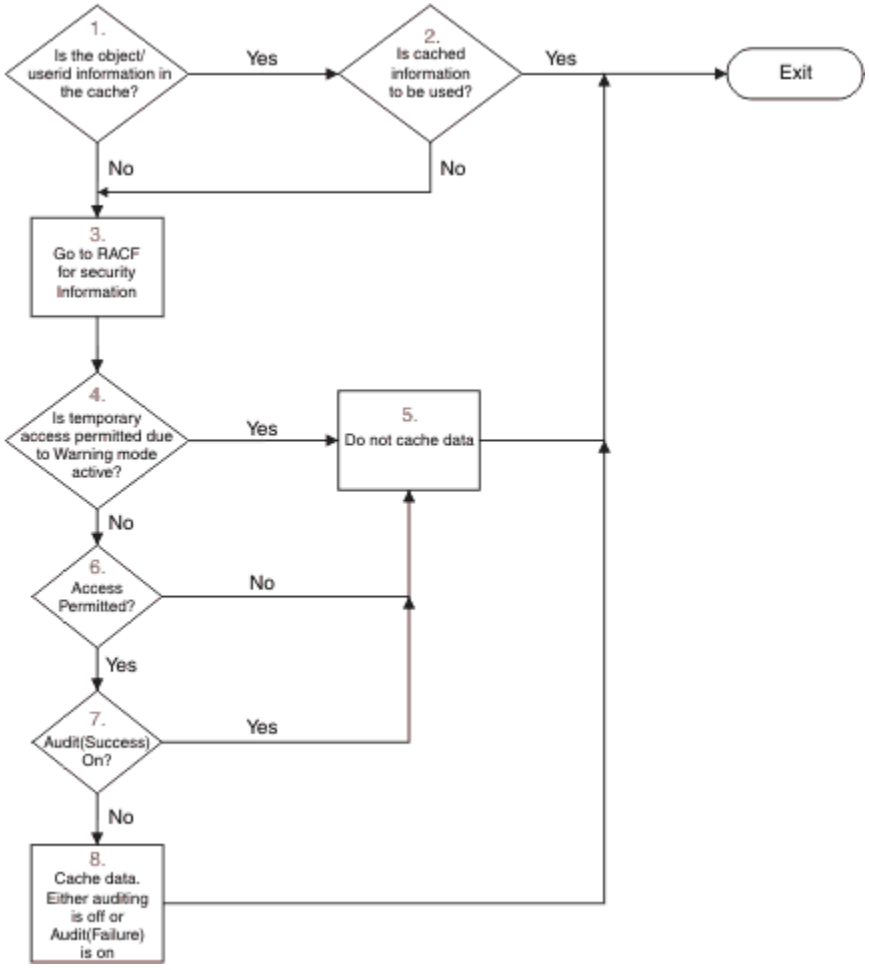
```
RLIST MQQUEUE (qmgr.SYSTEM.COMMAND.INPUT) GEN
```

a přijmout výsledky

```
CLASS      NAME
-----      ----
MQQUEUE    QP*.SYSTEM.COMMAND.*.** (G)
    AUDITING
    --------
    FAILURES(READ)
```

To označuje, že je zapnuto auditování. Další informace naleznete v příručce *z/OS Security Server RACF Auditor's Guide* a v příručce *z/OS Security Server RACF Command Language Reference*.

Obrázek 17 na stránce 245 shrnuje situace, ve kterých se informace o zabezpečení ukládají do mezipaměti a ve kterých se používají informace uložené v mezipaměti.



Obrázek 17. Logický tok pro ukládání do mezipaměti zabezpečení produktu IBM MQ

Změníte-li nastavení zabezpečení přidáním nebo odstraněním profilů přepínače ve třídách MQADMIN nebo MXADMIN, použijte jeden z těchto příkazů k dynamickému výběru těchto změn:

AKTUALIZOVAT ZABEZPEČENÍ (*)
AKTUALIZOVAT ZABEZPEČENÍ (MQADMIN)
AKTUALIZOVAT ZABEZPEČENÍ (MXADMIN)

To znamená, že můžete aktivovat nové typy zabezpečení nebo je deaktivovat, aniž byste museli restartovat správce front.

Z výkonnostních důvodů jsou to jediné třídy ovlivněné příkazem REFRESH SECURITY. Pokud měníte profil ve třídách MQCONN nebo MQCMDS, není nutné používat volbu REFRESH SECURITY.

Poznámka: Aktualizace třídy MQADMIN nebo MXADMIN není vyžadována, pokud změníte profil zabezpečení RESLEVEL.

Z výkonnostních důvodů použijte parametr REFRESH SECURITY tak často, jak je to možné, ideálně v době mimo špičku. Můžete minimalizovat počet obnov zabezpečení připojením uživatelů ke skupinám RACF , které jsou již v seznamu pro přístup k profilům IBM MQ , a nikoli k ukládání jednotlivých uživatelů do seznamů pro přístup. Tímto způsobem změníte spíše uživatele než profil prostředků. Můžete také RVERIFY SECURITY odpovídajícího uživatele místo obnovení zabezpečení.

Jako příklad REFRESH SECURITY předpokládejme, že definujete nové profily k ochraně přístupu do front začínajících řetězcem INSURANCE.LIFE ve správci front PRMQ. Použijte tyto příkazy RACF :

```
RDEFINE MQQUEUE PRMQ.INSURANCE.LIFE.** UACC(NONE)
PERMIT PRMQ.INSURANCE.LIFE.** ID(LIFEGRP) ACCESS(UPDATE)
```

Musíte zadat následující příkaz, abyste sdělili produktu RACF , že má aktualizovat informace o zabezpečení, které zadržuje, například:

```
SETROPTS RACLIST(MQQUEUE) REFRESH
```

Vzhledem k tomu, že tyto profily jsou generické, musíte produktu RACF sdělit, aby se aktualizování generických profilů pro MQQUEUE aktualizování. Příklad:

```
SETROPTS GENERIC(MQQUEUE) REFRESH
```

Pak je třeba pomocí tohoto příkazu sdělit správci front PRMQ, že se profily fronty změnily:

```
REFRESH SECURITY(MQQUEUE)
```

Aktualizace zabezpečení SSL/

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, aniž byste museli restartovat inicializátor kanálu.

z/OS *Zobrazení stavu zabezpečení*

Chcete-li zobrazit stav přepínačů zabezpečení a dalších ovládacích prvků zabezpečení, zadejte příkaz MQSC DISPLAY SECURITY.

Na následujícím obrázku je znázorněn 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 subsystém, příkaz, alternativní uživatele, proces, seznam názvů a zabezpečení fronty, které jsou aktivní na úrovni správce front, nikoli však na úrovni skupiny sdílení front. Připojení, prostředek příkazu a zabezpečení kontextu nejsou aktivní. Také ukazuje, že jsou aktivní časové limity ID uživatele a že každých 12 minut správce front zkontroluje ID uživatele, která nebyla použita v tomto správci front během 54 minut, a odebere je.

Poznámka: Tento příkaz zobrazí aktuální stav zabezpečení. Nenutně odráží aktuální stav profilů přepínačů definovaných pro RACFnebo stav tříd RACF . Např. profily přepínače se mohly změnit od posledního restartu tohoto správce front nebo příkazu REFRESH SECURITY.

z/OS Úlohy instalace zabezpečení pro produkt z/OS

Po instalaci a úpravě produktu IBM MQautorizujte spuštěné procedury úloh pro produkt RACF, autorizujte přístup k různým prostředkům a nastavte definice RACF . Volitelně můžete konfigurovat systém pro TLS.

Je-li produkt IBM MQ poprvé nainstalován a upraven, je třeba provést tyto úlohy související se zabezpečením:

1. Nastavení IBM MQ datové sady a zabezpečení systému pomocí:
   - Autorizace správce front byla spuštěna-procedura úlohy xxxxMSTR a distribuovaná fronta spustila-úloha xxxxCHIN , která má být spuštěna v rámci produktu RACF.
   - Autorizování přístupu k datovým sadám správce front.
   - Autorizující přístup k prostředkům pro jména uživatelů, která budou používat správce front a obslužné programy.
   - Autorizuje přístup pro ty správce front, kteří budou používat struktury seznamu prostředku Coupling Facility.
   - Autorizuje přístup pro ty správce front, kteří budou používat produkt Db2.
2. Nastavte definice RACF pro zabezpečení produktu IBM MQ .
3. Chcete-li použít protokol TLS (Transport Layer Security), připravte svůj systém k použití certifikátů a klíčů.

z/OS *Nastavení zabezpečení datové sady produktu IBM MQ for z/OS*

Existuje mnoho typů uživatelů IBM MQ . RACF umožňuje řídit jejich přístup k datovým sadám systému.

Možné uživatele datových sad produktu IBM MQ zahrnují následující entity:

- Samotný správce front.
- Inicializátor kanálu

- Administrátoři produktu IBM MQ , kteří potřebují vytvořit datové sady produktu IBM MQ , spouštět obslužné programy a podobné úlohy.
- Programátoři aplikací, kteří potřebují používat zakladače dodávané s produktem IBM MQ, obsahují datové sady, makra a podobné prostředky.
- Žádosti zahrnující jednu nebo více z těchto položek:
  - Dávkové úlohy
  - TSO uživatelé
  - Oblasti položek CICS
  - Oblasti položek IMS
- Datové sady CSQOUTX a CSQSNAP
- Dynamické fronty SYSTEM.CSQXCMD.*

Pro všechny tyto potenciální uživatele chraňte datové sady produktu IBM MQ pomocí produktu RACF.

Musíte také řídit přístup ke všem datovým sadám 'CSQINP'.

z/OS *RACF autorizace spuštěných procedur úloh*

Některé datové sady produktu IBM MQ jsou určeny pro výlučné použití správce front. Pokud chráníte své datové sady produktu IBM MQ pomocí produktu RACF, musíte také autorizovat spuštěnou úlohu správce front xxxxMSTRa postup spuštění distribuované fronty úloh xxxxCHINpomocí příkazu RACF. Chcete-li to provést, použijte třídu STARTED. Alternativně můžete použít tabulku spuštěných procedur (ICHRIN03), ale pak musíte provést IPL systému z/OS , aby se změny projevily.

Další informace najdete v příručce *z/OS Security Server RACF System Programmer's Guide*.

Identifikovaná ID uživatele produktu RACF musí mít požadovaný přístup k datovým sadám v proceduře spuštění úlohy. Například, pokud přidružíte proceduru spuštění úlohy správce front s názvem CSQ1MSTR s ID uživatele RACF QMGRCSQ1, musí mít ID uživatele QMGRCSQ1 přístup k prostředkům produktu z/OS , ke kterým má přístup správce front CSQ1 .

Také obsah pole GROUP v ID uživatele správce front musí být stejný jako obsah pole GROUP v profilu STARTED pro daného správce front. Pokud se obsah v každém poli GROUP neshoduje, pak se mu do systému nezabrání odpovídající ID uživatele. Tato situace způsobí, že produkt IBM MQ bude spuštěn s nedefinovaným ID uživatele a následně se uzavře kvůli narušení zabezpečení.

ID uživatelů produktu RACF přidružená k procedurám úlohy spuštěných 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 249 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 249 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 V 9.2.0 *Šifrování datových sad*

Datové sady produktu IBM MQ lze šifrovat pomocí z/OS šifrování datové sady, takže data jsou chráněna nebo z regulačních důvodů.

Můžete chránit všechny sady stránek, aktivní protokol, protokol archivace a zaváděcí datové sady BSDS s šifrováním datové sady produktu z/OS .

Upozornění: Sdílenou datovou sadu zpráv (SMDS) nelze chránit před šifrováním datové sady produktu z/OS pomocí produktu IBM MQ for z/OS 9.1.4 nebo starší verze.

Informace naleznete v části Důvěrnost dat v produktu IBM MQ for z/OS s šifrováním datové sady. Další informace viz.

z/OS *Nastavení zabezpečení prostředků produktu IBM MQ for z/OS*

Existuje mnoho typů uživatelů IBM MQ . Pomocí produktu RACF můžete řídit jejich přístup k prostředkům produktu IBM MQ .

Možnými uživateli prostředků produktu IBM MQ , jako jsou fronty a kanály, patří následující entity:

- Samotný správce front.
- Inicializátor kanálu

- Administrátoři produktu IBM MQ , kteří potřebují vytvořit datové sady produktu IBM MQ , spouštět obslužné programy a podobné úlohy
- Programátoři aplikací, kteří potřebují používat zakladače dodávané s produktem IBM MQ, obsahují datové sady, makra a podobné prostředky.
- Žádosti zahrnující jednu nebo více z těchto položek:
  - Dávkové úlohy
  - TSO uživatelé
  - Oblasti položek CICS
  - Oblasti položek IMS
- Datové sady CSQOUTX a CSQSNAP
- Dynamické fronty SYSTEM.CSQXCMD.*

Pro všechny tyto potenciální uživatele chraňte prostředky produktu IBM MQ pomocí produktu RACF. Konkrétně si všimněte, že iniciátor kanálu potřebuje přístup k různým prostředkům, jak je popsáno v “Aspekty zabezpečení pro inicializátor kanálu v systému z/OS” na stránce 256, a proto musí mít ID uživatele, pod kterým je spuštěna, oprávnění pro přístup k těmto prostředkům.

Pokud používáte skupinu sdílení front, správce front může interně vydávat různé příkazy, takže ID uživatele, které používá, musí mít autorizaci k vydávání těchto příkazů. Tyto příkazy jsou:

- DEFINE, ALTER a DELETE pro každý objekt, který má QSGDISP (GROUP)
- START a STOP CHANNEL pro každý kanál, který se používá se CHLDISP (SHARED)

z/OS *Konfigurace systému z/OS pro použití TLS*

Toto téma se používá jako příklad konfigurace produktu IBM MQ for z/OS s protokolem TLS (Transport Layer Security) pomocí příkazů RACF .

Chcete-li pro zabezpečení kanálu použít TLS, je třeba ve vašem systému provést několik úloh. (Podrobné informace o použití příkazů RACF pro certifikáty a úložiště klíčů (klíčové řetězce) naleznete v tématu Práce s TLS v systému z/OS .)

1. Vytvořte svazek klíčů v produktu RACF pro uložení všech klíčů a certifikátů pro váš systém pomocí příkazu RACDCERT RACF . Příklad:

   ```
   RACDCERT ID(CHINUSER) ADDRING(QM1RING)
   ```

   ID musí být buď ID uživatele adresního prostoru kanálu kanálu, nebo ID uživatele, které chcete vlastnit svazek klíčů, pokud se má jednat o sdílený svazek klíčů.
2. Vytvořte digitální certifikát pro každého správce front pomocí příkazu RACF RACDCERT.

   Jmenovka certifikátu musí být buď hodnota atributu IBM MQ **CERTLABL** , je-li nastavena, nebo výchozí `ibmWebSphereMQ` s názvem správce front nebo skupiny sdílení front s připojeným názvem. Podrobnosti najdete v tématu Digitální certifikáty certifikátu . V tomto příkladě je to `ibmWebSphereMQQM1`.

   Příklad:

   ```
   RACDCERT ID(USERID) GENCERT
   SUBJECTSDN(CN('username') O('IBM') OU('departmentname') C('England'))
   WITHLABEL('ibmWebSphereMQQM1')
   ```
3. Připojte certifikát v produktu RACF k souboru svazku klíčů pomocí příkazu RACF RACDCERT. Příklad:

```
RACDCERT CONNECT(ID(USERID) LABEL('ibmWebSphereMQQM1') RING(QM1RING))
CONNECT ID(CHINUSER)
```

Je také třeba připojit všechny příslušné certifikáty podepisujících subjektů (od certifikační autority) ke klíči 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 použijte příkaz IBM MQ ALTER QMGR a určete úložiště klíčů, na které má správce front odkazovat. Je-li například svazek klíčů vlastněný 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 orgánům odvolávat certifikáty, které již nemohou být důvěryhodné. Seznamy CRL jsou uloženy na serverech LDAP. Chcete-li získat přístup na tento seznam na serveru LDAP, musíte nejprve vytvořit objekt AUTHINFO typu 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 na serveru LDAP, takže pole LDAPUSER a LDAPPWD nejsou nezbytná.

Dále umístěte objekt AUTHINFO do seznamu názvů pomocí příkazu IBM MQ DEFINE NAMELIST. Příklad:

```
DEFINE NAMELIST(LDAPNL) NAMES(LDAP1)
```

Nakonec přidružte seznam názvů k jednotlivým správcům front pomocí příkazu IBM MQ ALTER QMGR. Příklad:

```
ALTER QMGR SSLCRLNL(LDAPNL)
```

6. Set up your queue manager to run TLS calls, using the IBM MQ ALTER QMGR command. Toto definuje podúlohy serveru, které obsluhují pouze volání SSL, což ponechá normální dispečery pokračovat ve zpracování jako normální, aniž by to bylo ovlivněno žádným voláním SSL. Musíte mít alespoň dva z těchto podúloh. Příklad:

```
ALTER QMGR SSLTASKS(8)
```

   Tato změna se projeví až po restartování inicializátoru kanálu.

7. Uveďte specifikaci šifry, která má být použita pro každý kanál, pomocí příkazu IBM MQ DEFINE CHANNEL nebo ALTER CHANNEL. 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 ověření kanálu v QSG

Záznamy ověření kanálu se vztahují na správce front, kterého jsou vytvořeny, nebudou sdíleny v rámci skupiny sdílení front (QSG). Proto jsou-li všichni správci front ve skupině sdílení front povinni mít stejná pravidla, je třeba provést některé řízení tak, aby byla zachována konzistence všech pravidel.

1. Vždy přidejte volbu CMDSCOPE(*) do všech příkazů SET CHLAUTH . Tento příkaz odešle příkaz všem spuštěným správcům front ve skupině sdílení front.
2. Použijte příkaz DISPLAY CHLAUTH s volbou CMDSCOPE(*) a potom analyzujte odezvy, abyste zjistili, zda jsou záznamy stejné od všech správců front. Je-li nalezena nekonzistence, lze zadat příkaz SET CHLAUTH obsahující stejné pravidlo s CMDSCOPE(*) nebo CMDSCOPE(*qmgr-name*).
3. Přidejte člena do zřetězení CSQINP2 správce front (viz Inicializační příkazy), které mají úplnou sadu pravidel. Ty budou načteny jako součást procesu inicializace správce front. Pokud příkaz SET CHLAUTH používá příkaz ACTION(ADD) , bude pravidlo přidáno pouze v případě, že neexistuje. Použití ACTION(REPLACE) nahradí existující pravidlo, pokud již existuje, nebo jej přidat, pokud se tak nestane. Stejný člen by pak mohl být umístěn ve zřetězení CSQINP2 všech správců front ve skupině sdílení front.
4. Chcete-li extrahovat pravidla z jednoho správce front pomocí volby MAKEDEF nebo MAKEREP , použijte obslužný program CSQUTIL (viz část Vydávání příkazů do IBM MQ (COMMAND)). Pak 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 standardní ovládací prvky auditování produktu RACF . Produkt IBM MQ neshromažďuje žádné statistické údaje zabezpečení. Jediné statistiky jsou ty, které mohou být vytvářeny auditováním.

Auditování RACF může být založeno na:

- ID uživatelů
- Třídy prostředků
- Profily

Další informace najdete v příručce *z/OS Security Server RACF Auditor's Guide*.

Poznámka: Auditování degraduje výkon, čím více auditování implementujete, tím více je degradováno. Jedná se také o úvahu pro použití volby VAROVÁNÍ RACF .

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 253.

```
       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 naleznete v příručce *z/OS Security Server RACF Auditor's Guide*.

z/OS Přizpůsobení zabezpečení

Chcete-li změnit způsob zabezpečení produktu IBM MQ , je třeba provést toto nastavení prostřednictvím uživatelské procedury SAF (ICHRFR00) nebo skončit ve správci externích zabezpečení.

Další informace o uživatelských procedurách produktu RACF naleznete v příručce *z/OS Security Server RACROUTE Macro Reference* .

Poznámka: Protože program IBM MQ optimalizuje volání do ESM, požadavky RACROUTE nemusí být prováděny například při každém otevření určité fronty konkrétním uživatelem.

z/OS Zprávy o narušení zabezpečení v systému z/OS

Narušení zabezpečení je označeno návratovým kódem MQRC_NOT_AUTHORIZED v aplikačním programu nebo prostřednictvím zprávy v protokolu úlohy.

Návratový kód operace MQRC_NOT_AUTHORIZED může být vrácen do aplikačního programu z následujících důvodů:

- Uživateli není dovoleno připojit se ke správci front. V takovém případě obdržíte zprávu ICH408I v protokolu úlohy Batch/TSO, CICSnebo IMS .
- Přihlášení uživatele do správce front se nezdařilo, protože například ID uživatele úlohy není platné nebo je to vhodné, nebo ID uživatele úlohy nebo alternativní ID uživatele není platné. Jedno nebo více z těchto ID uživatelů nemusí být platné, protože byly odebrány nebo odstraněny. V tomto případě získáte zprávu ICHxxxx a případně zprávu IRRxxxx v protokolu úlohy správce front, kde došlo k selhání při 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 nebo úlohy nemá přístup k alternativnímu ID uživatele. Pro toto selhání obdržíte zprávu o narušení v protokolu úlohy příslušného správce front.
- Volba kontextu byla použita nebo je odvozena z otevření přenosové fronty pro výstup, ale ID uživatele úlohy nebo případně úloha nebo alternativní ID uživatele nemá přístup k volbě kontextu. V takovém případě je do protokolu úlohy příslušného správce front vložena zpráva o narušení.
- Neautorizovaný uživatel se pokusil o přístup k zabezpečenému objektu správce front, například k frontě. V tomto případě je do protokolu úlohy příslušného správce front vložena zpráva ICH408I pro narušení. Toto porušení může být způsobeno úlohou nebo, je-li to vhodné, úlohou nebo alternativním ID uživatele.

Zprávy o narušení pro zabezpečení příkazů a zabezpečení prostředků příkazů lze také najít v protokolu úlohy správce front.

Pokud zpráva o narušení ICH408I zobrazuje název úlohy správce front a nikoli ID uživatele, je obvykle výsledkem 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, komu je povoleno používat prázdná alternativní ID uživatelů, a to tak, že zkontrolujete seznam pro přístup k profilu MQADMIN hlq.ALTERNATE.USER.-BLANK-.

Zprávu o narušení ICH408I lze také vygenerovat příkazem:

- Příkaz odesílaný do vstupní fronty příkazového řádku bez kontextu. Uživatelské programy, které zapisují do vstupní fronty systémových příkazů, by vždy měly používat volbu kontextu. Další informace viz téma “Profily pro zabezpečení kontextu” na stránce 211.
- Když úloha přistupující k prostředku IBM MQ nemá přidružené ID uživatele nebo pokud adaptér IBM MQ nemůže extrahovat ID uživatele z prostředí adaptéru.

Zprávy o narušení mohou být vydávány také v případě, že používáte skupinu sdílení front i zabezpečení na úrovni správce front. Můžete získat zprávy označující, že nebyl nalezen žádný profil na úrovni správce front, ale stále mu bude udělen přístup z důvodu profilu 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   )
```

z/OS Co dělat, pokud je přístup povolen nebo nepovolen nesprávně

Kromě kroků podrobně popsaných v příručce *z/OS Security Server RACF Security Administrator's Guide*použijte tento kontrolní seznam, pokud se zdá, že přístup k prostředku je nesprávně řízen.

- Jsou profily přepínačů správně nastaveny?
  - Je RACF aktivní?
  - Jsou třídy IBM MQ RACF instalovány a aktivní?

    Chcete-li to zkontrolovat, použijte příkaz RACF SETROPTS LIST.
  - Chcete-li zobrazit aktuální stav přepínače ze správce front, použijte příkaz IBM MQ DISPLAY SECURITY.
  - Zkontrolujte profily přepínačů ve třídě MQADMIN.

    Pro tento příkaz použijte příkazy RACF , SEARCH a RLIST.
  - Znovu zkontrolujte profily přepínačů RACF zadáním příkazu IBM MQ REFRESH SECURITY (MQADMIN).
- Změnil se profil prostředků RACF ? Má se například změněn univerzální přístup na profil nebo je změněn seznam přístupů profilu?
  - Je profil generický?

    Je-li tomu tak, zadejte příkaz RACF SETROPTS GENERIC (název_třídy) OBNOVIT.
  - Aktualizovali jste zabezpečení tohoto správce front?

    Je-li to nutné, zadejte příkaz RACF SETROPTS RACLIST (název_třídy) OBNOVIT.

    Je-li to nutné, zadejte příkaz IBM MQ REFRESH SECURITY (*).
- Změnila se definice RACF uživatele? Například, byl uživatel připojen k nové skupině nebo má oprávnění k přístupu uživatele zrušeno oprávnění?
  - Ověřili jste uživatele zadáním příkazu IBM MQ RVERIFY SECURITY (userid)?
- Jsou v důsledku RESLEVEL vynechány kontroly zabezpečení?
  - Zkontrolujte přístup ID uživatele s připojením k profilu RESLEVEL. Použijte záznamy auditu RACF , abyste určili, na kterou hodnotu RESLEVEL je nastavena.
  - V případě kanálů pamatujte na to, že úroveň přístupu, kterou ID uživatele iniciátoru kanálu má na RESLEVEL, zdědí všechny kanály, takže úroveň přístupu, jako např. ALTER, která způsobí, že všechny kontroly budou vynechány, způsobí, že budou všechny kanály vynechány pro všechny kanály.
  - Pokud spouštíte produkt CICS, zkontrolujte nastavení RESESEC transakce.
  - Pokud byla při připojení uživatele změněna hodnota RESLEVEL, musí se před novým nastavením RESLEVEL znovu odpojit a znovu připojit.
- Používáte skupiny sdílení front?
  - Používáte-li skupinu sdílení front i úroveň zabezpečení správce front, zkontrolujte, zda jste definovali všechny správné profily. Není-li profil správce front definován, odešle se do protokolu zpráva s informací o tom, že profil nebyl nalezen.
  - Použili jste kombinaci nastavení přepínače, která není platná, takže byla nastavena úplná kontrola zabezpečení?

- Potřebujete definovat přepínače zabezpečení, chcete-li přepsat některá nastavení skupiny sdílení front pro správce front?
- Má profil na úrovni správce front přednost před profilem úrovně skupiny sdílení front?

z/OS Aspekty zabezpečení pro inicializátor kanálu v systému z/OS

Pokud používáte zabezpečení na úrovni prostředků v distribuovaném prostředí řazení do fronty, potřebuje adresní prostor Inicializátor kanálu odpovídající přístup k různým prostředkům produktu IBM MQ .
K vytvoření algoritmu ochrany heslem můžete použít program Integrated Cryptographic Support Facility (ICSF).

Použití zabezpečení prostředků

Pokud používáte zabezpečení prostředků, zvažte následující body, pokud používáte distribuované ukládání do fronty:

systémových front
Adresní prostor inicializátoru kanálu potřebuje přístup RACF UPDATE k systémovým frontám uvedeným v seznamu “Zabezpečení systémové fronty” na stránce 200a ke všem cílovým frontám uživatele a frontám nedoručených zpráv (viz “Zabezpečení fronty nedoručených zpráv” na stránce 199).

Přenosové fronty
Adresní prostor inicializátoru kanálu vyžaduje přístup ALTER ke všem přenosovým frontám uživatele.

zabezpečení kontextu
ID uživatele kanálu (a ID uživatele MCA, je-li zadán) potřebují RACF CONTROL přístup k profilům hlq.CONTEXT.queuename ve třídě MQADMIN. V závislosti na profilu RESLEVEL může ID uživatele kanálu také potřebovat CONTROL přístup k těmto profilům.

Všechny kanály vyžadují přístup CONTROL k souboru MQADMIN hlq.CONTEXT. profil fronty nedoručených zpráv. Všechny kanály (ať již iniciující nebo odpovídající) mohou generovat sestavy a v důsledku toho potřebují přístup CONTROL k profilu hlq.CONTEXT.reply-q .

Kanály SENDER, CLUSSDR a SERVER vyžadují přístup CONTROL k profilům hlq.CONTEXT.xmit-queue-name , protože zprávy mohou být vloženy do přenosové fronty, aby se kanál mohl ukončit postupně.

Poznámka: Pokud má ID uživatele kanálu nebo skupina RACF , ke které je připojeno ID uživatele kanálu, přístup CONTROL nebo ALTER k souboru hlq.RESLEVEL, nejsou pro iniciátor kanálu nebo některé jeho kanály žádné kontroly prostředků.

Další informace viz “Profily pro zabezpečení kontextu” na stránce 211 “RESLEVEL a připojení inicializátoru kanálu” na stránce 231 a “ID uživatelů pro kontrolu zabezpečení v systému z/OS” na stránce 233 .

CSQINPX
Pokud používáte vstupní datovou sadu CSQINPX, pak iniciátor kanálu také potřebuje přístup READ ke CSQINPX a přístup UPDATE k datové sadě CSQOUTX a dynamické fronty 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 193.

Datové sady
Adresní prostor inicializátoru kanálu potřebuje odpovídající přístup k datovým sadám správce front, viz “Autorizace přístupu k datovým sadám” na stránce 248.

Příkazy
Příkazy s distribuovanými frontami (například DEFINE CHANNEL, START CHINIT, START LISTENER a další kanálové příkazy) musí mít nastaven odpovídající sadu zabezpečení příkazů, viz Tabulka 49 na stránce 214.

Pokud používáte skupinu sdílení front, iniciátor kanálu může interně vydat různé příkazy, takže ID uživatele, které používá, musí mít autorizaci k vydávání těchto příkazů. Tyto příkazy jsou START a STOP CHANNEL pro každý kanál, který se používá se CHLDISP (SHARED).

Pokud PSMODE správce front není VYPNUTÝ, musí mít inicializátor kanálu přístup READ k příkazu DISPLAY PUBSUB.

Zabezpečení kanálu

Kanály, zejména zásobníky a připojení k serveru, vyžadují nastavení zabezpečení. Další informace naleznete v dokumentu "ID uživatelů pro kontrolu zabezpečení v systému z/OS" na stránce 233 .

K zajištění zabezpečení na kanálech můžete také použít protokol TLS (Transport Layer Security). Další informace o použití TLS v produktu IBM MQviz "Protokoly zabezpečení TLS v produktu IBM MQ" na stránce 22 .

Další informace o zabezpečení připojení k serveru najdete v příručce "Řízení přístupu pro klienty" na stránce 96 .

ID uživatelů

ID uživatelů popsaná v tématech "ID uživatele použitá inicialiátorem kanálu" na stránce 236 a "ID uživatelů použitá agentem front v rámci skupiny" na stránce 240 potřebují následující přístup:

- RACF UPDATE access to the appropriate destination queues and the dead-letter queue
- RACF CONTROL přístup k profilu produktu `hlq.CONTEXT.queuename` , pokud se provádí kontrola kontextu na přijímači.
- Přiměřený přístup k souboru hlq.ALTERNATE.USER.userid , které mohou potřebovat použít.
- Pro klienty je vhodný přístup RACF k prostředkům, které mají být použity.

Zabezpečení APPC

Používáte-li přenosový protokol LU 6.2 , nastavte odpovídající zabezpečení APPC. (Například použijte třídu APPCLU RACF .) Informace o nastavení zabezpečení pro APPC naleznete v následujících příručkách:

- *z/OS V1R2.0 Plánování MVS: Správa APPC*
- Publikace *Multiplatform APPC Configuration Guide*, publikace IBM Redbooks

Odchozí přenosy používají volbu protokolu APPC "SECURITY (SAME)" . V důsledku toho je ID uživatele adresního prostoru iniciátoru kanálu a jeho výchozí profil (RACF GROUP) přenášena po síti k přijímači s indikátorem, že ID uživatele již bylo ověřeno (ALREADYV).

Je-li přijímající strana také z/OS, ID uživatele a profil jsou ověřeny pomocí APPC a ID uživatele se předkládá k přijímacímu kanálu a používá se jako ID uživatele kanálu.

V prostředí, ve kterém správce front používá APPC ke komunikaci s jiným správcem front ve stejném nebo v jiném systému z/OS , je třeba zajistit, aby:

- Definice VTAM pro komunikující LU určuje SETACPT (ALREADYV).
- Existuje profil RACF APPCLU pro připojení mezi jednotkami LU, které uvádí CONVSEC (ALREADYV)

Změna nastavení zabezpečení

Je-li úroveň přístupu RACF , která má ID uživatele kanálu nebo jméno uživatele MCA, změněna, projeví se tato změna pouze pro nové popisovače objektů (tj. nové `MQOPEN`) pro cílovou frontu. Časy, kdy jsou otevřené fronty MCaAs a zavírají fronty; pokud je kanál již spuštěn, když se provádí taková změna přístupu, může agent MCA pokračovat v vkládání zpráv do cílové fronty s použitím existujícího zabezpečeného přístupu k ID uživatelů, nikoli k aktualizovanému zabezpečovanému přístupu. Zastavení a restartování kanálů k vynucení aktualizované úrovně přístupu se tomuto scénáři vyhýbá.

automatický restart

Pokud k restartování inicializátoru kanálu používáte produkt z/OS Automatic Restart Manager (ARM), musí být ID uživatele přidruženého k adresnímu prostoru XCFAS autorizováno pro zadání příkazu IBM MQ START CHINIT.

Použití programu ICSF (Integrated Cryptographic Service Facility)

Inicializátor kanálu může použít službu ICSF k vygenerování náhodného čísla při zavedení algoritmu ochrany heslem pro zamaskování hesel procházejících přes kanály klienta, pokud se TLS nepoužívá. Proces generování náhodného čísla se nazývá *entropie*.

Pokud jste nainstalovali 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 heslem není tak zabezpečený, jak by mohl být. Můžete však pokračovat ve svém procesu. V běhovém prostředí není žádný jiný dopad.

Pokud nemáte nainstalovanou funkci produktu z/OS , bude inicializátor kanálu automaticky používat STCK.

Notes:

1. Použití ICSF pro entropii generuje více náhodných sekvencí než použití STCK.
2. Pokud spustíte ICSF, musíte restartovat inicializátor kanálu.
3. ICSF se požaduje pro určité CipherSpecs. Pokusíte-li se použít některou z těchto CipherSpecs a nemáte-li nainstalované služby ICSF, obdržíte zprávu CSQX629E.

z/OS Zabezpečení klastrů 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 potřebují odpovídající sadu zabezpečení.

K ověření kanálů klastru (jako u konvenčních kanálů) můžete použít ID uživatele MCA, záznamy ověření kanálu, TLS a uživatelské procedury zabezpečení. Záznamy ověření kanálu nebo uživatelská procedura zabezpečení související s přijímacím kanálem klastru musí zkontrolovat, zda má vzdálený správce front povolen přístup k frontám klastru správce front serveru. Můžete začít používat podporu klastrů produktu IBM MQ , aniž byste změnili existující zabezpečení přístupu k frontě. Musíte však povolit ostatním správcům front v klastru, aby zapisoval do systému SYSTEM.CLUSTER.COMMAND.QUEUE , pokud se mají připojit ke klastru.

Podpora klastrů produktu IBM MQ neposkytuje mechanizmus k omezení člena klastru pouze na roli klienta. V důsledku toho si musíte být jisti, že důvěřujete všem správcům front, které povolíte do klastru. Pokud některý správce front v klastru vytvoří frontu s určitým názvem, může pro tuto frontu přijímat zprávy bez ohledu na to, zda aplikace vkládá zprávy do této fronty nebo ne.

Chcete-li omezit členství klastru, proveďte stejnou akci, jakou byste měli provést, abyste zabránili připojení správců front k přijímacím kanálům. Členství v klastru omezíte tím, že použijete záznamy ověření kanálu nebo napíšete uživatelský program zabezpečení do přijímacího kanálu. Můžete také napsat ukončovací program, který zabrání neoprávněným správcům front zapisovat do SYSTEM.CLUSTER.COMMAND.QUEUE.

Poznámka: Doporučuje se, aby aplikace neotvírejte SYSTEM.CLUSTER.TRANSMIT.QUEUE přímo. Také se nedoporučuje povolovat aplikaci, aby přímo otevřela jakoukoli jinou přenosovou frontu.

Používáte-li zabezpečení prostředků, zvažte kromě aspektů obsažených v produktu “Aspekty zabezpečení pro inicializátor kanálu v systému z/OS” na stránce 256následující body:

systémových front
Inicializátor kanálu potřebuje RACF ALTER pro přístup k následujícím frontám systému:

- SYSTEM.CLUSTER.COMMAND
- SYSTEM.CLUSTER.TRANSMIT.QUEUE.

a přístup UPDATE k SYSTEM.CLUSTER.REPOSITORY.QUEUE

Potřebuje také přístup READ k libovolným seznamům názvů, které se používají pro klastrování.

Příkazy
Nastavte odpovídající zabezpečení příkazu (jak je popsáno v tématu Tabulka 49 na stránce 214). v případě příkazů podpory klustru (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 produktu IBM MQ s produktem IMS

Toto téma popisuje, jak naplánovat požadavky na zabezpečení při použití produktu IBM MQ s produktem IMS.

Použití třídy OPERCMDS

Pokud používáte produkt RACF k ochraně prostředků ve třídě OPERCMDS, ujistěte se, že ID uživatele přidružené k adresnímu prostoru správce front produktu IBM MQ má oprávnění k vydávání příkazu MODIFY pro libovolný systém IMS , ke kterému se může připojit.

Aspekty zabezpečení pro most IMS

Existují čtyři aspekty, které musíte zvážit při rozhodování o svých požadavcích na zabezpečení mostu IMS :

- Jaká autorizace zabezpečení je zapotřebí pro připojení IBM MQ k IMS
- Kolik kontroly zabezpečení se provádí u aplikací, které používají most pro přístup k produktu IMS
- Které IMS prostředky jsou tyto aplikace povoleny pro použití
- Jaké oprávnění má být použito pro zprávy, které jsou vloženy do mostu a jsou k ní

Při definování požadavků zabezpečení pro most IMS je třeba vzít v úvahu následující skutečnosti:

- Zprávy procházející přes most mohly pocházet z aplikací na platformách, které nenabízejí silné ochranné prvky.
- Zprávy procházející přes most mohou pocházet z aplikací, které nejsou řízeny stejným podnikem nebo organizací.

z/OS *Aspekty zabezpečení pro připojení k produktu IMS*

Udělte ID uživatele pro přístup k adresnímu prostoru správce front produktu IBM MQ přístup k skupině OTMA.

Most IMS je klientem OTMA. Připojení k produktu IMS pracuje pod ID uživatele adresního prostoru správce front produktu IBM MQ . Toto je obvykle definováno jako člen spuštěné skupiny úloh. Tomuto ID uživatele musí být udělen přístup ke skupině OTMA (není-li nastavení /SECURE OTMA nastaveno na hodnotu NONE).

Chcete-li to provést, definujte následující profil ve třídě FACILITY:

```
IMSXCF.xcfgname.mqxcfmname
```

Kde `xcfgname` je název skupiny XCF a `mqxcfmname` je název členu XCF produktu IBM MQ.

Do tohoto profilu je třeba udělit oprávnění pro čtení ID uživatele správce front produktu IBM MQ .

Poznámka:

1. Změníte-li oprávnění ve třídě FACILITY, musíte vydat příkaz RACF SETROPTS RACLIST (FACILITY) REFRESH, aby se změny aktivovaly.
2. Pokud profil hlq.NO.SUBSYS.SECURITY ve třídě MQADMIN existuje, není předáváno ID uživatele produktu IMS a připojení selže, pokud nastavení /SECURE OTMA není NONE.

z/OS *Řízení přístupu k aplikacím pro most IMS*

Definujte profil RACF ve třídě FACILITY pro každý systém IMS . Udělte odpovídající úroveň přístupu k ID uživatele správce front produktu IBM MQ .

Pro každý systém IMS , ke kterému se most IMS připojuje, můžete definovat následující profil RACF ve třídě FACILITY, abyste určili, kolik kontroly zabezpečení se provádí pro každou zprávu předanou do systému IMS .

```
IMSXCF.xcfgname.imsxcfmname
```

Kde `xcfgname` je název skupiny XCF a `imsxcfmname` je název členu XCF pro IMS. (Pro každý systém IMS je třeba definovat samostatný profil.)

Úroveň přístupu, kterou povolíte pro ID uživatele správce front produktu IBM MQ v tomto profilu, je vrácena systému IBM MQ , pokud se most IMS připojuje k produktu IMSa označuje úroveň zabezpečení vyžadovanou při následných transakcích. V případě následných transakcí IBM MQ vyžádá příslušné služby z produktu RACF a, je-li ID uživatele autorizováno, předá zprávu do produktu IMS.

OTMA nepodporuje příkaz IMS /SIGN; produkt IBM MQ však umožňuje nastavit kontrolu přístupu pro každou zprávu, aby bylo možné povolit implementaci potřebné úrovně řízení.

Mohou být vráceny následující informace o úrovni přístupu:

NEBYL NALEZEN
Tyto hodnoty označují, že je vyžadováno maximální zabezpečení, tj. ověření je povinné pro každou transakci. Je provedena kontrola za účelem ověření, zda ID uživatele zadané v poli *UserIdentifier* struktury MQMD a heslo nebo PassTicket v poli *Ověřovatel* struktury MQIIH jsou známy produktu RACFa jsou platnou kombinací. UTOKEN se vytvoří s heslem nebo PassTicketa předá se do IMS ; UTOKEN se neukládají do mezipaměti.

Poznámka: Pokud profil hlq.NO.SUBSYS.SECURITY existuje ve třídě MQADMIN, tato úroveň zabezpečení přepíše všechny definice definované v profilu.

READ (čtení)
Tato hodnota indikuje, že má být provedeno stejné ověření jako pro `NONE` za následujících okolností:

- První, kdy je zjištěno určité ID uživatele
- Když bylo zjištěno ID uživatele před tím, než se položka UTOKEN uložená v mezipaměti nevytvořila pomocí hesla nebo PassTicket

Produkt IBM MQ vyžaduje v případě potřeby volbu UTOKEN a předává je produktu IMS.

Poznámka: Pokud byl vydán požadavek na opětovné ověření zabezpečení, jsou všechny informace uložené v mezipaměti ztraceny a UTOKEN je požadován při prvním výskytu každého ID uživatele.

AKTUALIZOVAT
Kontrola se provede, že ID uživatele v poli *UserIdentifier* struktury MQMD je známé jako RACF.

Společnost UTOKEN je sestavena a předána do produktu IMS ; UTOKEN se ukládá do mezipaměti.

ŘÍZENÍ/ZMĚNA
Tyto hodnoty indikují, že pro ID uživatelů tohoto systému IMS není třeba poskytnout žádné zabezpečení UTOKENs zabezpečení. (Tuto volbu byste pravděpodobně používali pouze pro vývojový a testovací systém.)

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 produkt IBM MQ připojí k produktu IMSa trvá po dobu trvání připojení. Chcete-li změnit úroveň zabezpečení, je třeba změnit přístup k profilu zabezpečení a poté se přemostění zastavit a znovu spustit (například zastavením a restartováním OTMA).
2. Změníte-li oprávnění ve třídě FACILITY, musíte vydat příkaz RACF SETROPTS RACLIST (FACILITY) REFRESH, aby se změny aktivovaly.
3. Můžete použít heslo nebo PassTicket, ale musíte mít na paměti, že most IMS nešifruje data. Informace o použití PassTicketsviz "Použití RACF PassTickets v záhlaví IMS" na stránce 262.
4. Některé z těchto výsledků mohou být ovlivněny nastavením zabezpečení v produktu IMSpomocí příkazu /SECURE OTMA.
5. Informace UTOKEN uložené v mezipaměti jsou drženy po dobu trvání definovanou parametry INTERVAL a TIMEOUT příkazu IBM MQ ALTER SECURITY.
6. Volba WARNING RACF nemá žádný vliv na profil IMSXCF.xcfgname.imsxcfmname . Jeho použití nemá vliv na úroveň uděleného přístupu a žádné zprávy RACF WARNING se nevytvoří.

z/OS *Kontrola zabezpečení na systému IMS*

Zprávy, které procházejí přes most, obsahují informace o zabezpečení. Provedli se kontroly zabezpečení na základě nastavení příkazu IMS /SECURE OTMA.

Každá zpráva 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 struktura MQIIH přítomná)
- Hodnota UTOKEN (pokud nemá podsystém IBM MQ přístup CONTROL nebo ALTER k příslušnému profilu `IMSXCF.xcfgname.imsxcfmname`)

Provedla se kontrola zabezpečení na nastavení příkazu IMS /SECURE OTMA, jak je uvedeno níže:

/SECURE OTMA NONE
Pro transakci nejsou provedeny žádné kontroly zabezpečení.

/ZABEZPEČIT KONTROLU OTMMA
Pole *UserIdentifier* struktury MQMD je předáno příkazu IMS pro kontrolu transakcí nebo kontroly příkazů.

Položka ACEE (Accessor Environment Element) je vestavěna v řídicí oblasti IMS .

/SECURE OTMA FULL
Pole *UserIdentifier* struktury MQMD je předáno příkazu IMS pro kontrolu transakcí nebo kontroly příkazů.

ACEE je postaven v IMS závislé oblasti a také v řídicí oblasti IMS .

/SECURE OTMA PROFIL
Pole *UserIdentifier* struktury MQMD je předáno příkazu IMS pro kontrolu transakcí nebo oprávnění k příkazům.

Pole *SecurityScope* ve struktuře MQIIH se používá k určení, zda má být v IMS závislé oblasti a oblasti ovládacího prvku sestavované ACEE sestavované.

Poznámka:

1. Pokud změníte oprávnění ve třídě TIMS nebo CIMS nebo přidružené třídy skupin GIMS nebo DIMS, musíte pro aktivaci změn vydat následující příkazy IMS :
   - /MODIFY PREPARE RACF
   - /UPRAVIT POTVRZENÍ

2. Pokud nepoužíváte /SECURE OTMA PROFILE, bude ignorována libovolná hodnota uvedená v poli *SecurityScope* struktury MQIIH.

z/OS *Kontrola zabezpečení provedená pomocí mostu IMS*

Různí oprávnění se používají v závislosti na prováděné akci.

Když most vloží nebo získá zprávu, použijí se následující oprávnění:

Získání zprávy z fronty mostu
Neprovedou 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 v původní zprávě.

Vložení zprávy do fronty nedoručených zpráv
Neprovedou se žádné kontroly zabezpečení.

Poznámka:

1. Změníte-li profily tříd produktu IBM MQ , je třeba provést aktivaci změn zadáním příkazu IBM MQ REFRESH SECURITY (*).
2. Pokud změníte oprávnění uživatele, musíte pro aktivaci této změny vydat příkaz MQSC RVERIFY SECURITY.

z/OS *Použití RACF PassTickets v záhlaví IMS*

PassTicket můžete použít místo hesla v záhlaví IMS .

Pokud chcete použít PassTicket místo hesla v záhlaví IMS (MQIIH), uveďte jméno aplikace, proti které je PassTicket validován v atributu PASSTKTA definice STGCLASS fronty mostu IMS , do které má být zpráva směrována.

Je-li hodnota PASSTKTA ponechána prázdná, musíte zařídit, 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, cílového názvu aplikace a tajného klíče. Jedná se o 8bajtovou hodnotu obsahující velká písmena a číslice. Lze jej použít pouze jednou a je platný po dobu 20 minut. Pokud je PassTicket generován lokálním systémem RACF , RACF pouze kontroluje, zda profil existuje a ne, že má uživatel oprávnění k tomuto profilu. Pokud byl PassTicket generován na vzdáleném systému, produkt RACF ověří přístup ID uživatele k profilu. Informace o úplných informacích o PassTicketsviz příručka *z/OS SecureWay Security Server RACF Security Administrator's Guide*.

PassTickets v záhlaví IMS se dává RACF do IBM MQ, ne IMS.

z/OS Migrace správce front z/OS na smíšenou velikost písmen

Chcete-li provést migraci správce front do zabezpečení se smíšenými případy, postupujte podle následujících kroků. Přezkoumejte úroveň produktu zabezpečení, který používáte, a aktivujte nové třídy externího správce zabezpečení produktu IBM MQ . Spuštěním příkazu **REFRESH SECURITY** aktivujte profily smíšeného případu.

Než začnete

1. Ujistěte se, že jsou aktivovány všechny externí třídy správce zabezpečení produktu IBM MQ .
2. Ujistěte se, že je správce front spuštěn.

Informace o této úloze

Chcete-li převést správce front na zabezpečení se smíšenými případy, postupujte takto.

Postup

1. Okopírujte všechny existující profily a úrovně přístupu z tříd s velkými písmeny na ekvivalentní třídu externího správce zabezpečení smíšeného případu.
   a) `MQADMIN` na `MXADMIN`.
   b) `MQPROC` na `MXPROC`.
   c) `MQNLIST` na `MXNLIST`.
   d) `MQQUEUE` na `MXQUEUE`.
2. Změňte hodnotu atributu správce front `SCYCASE` na `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 se smíšenými případy s použitím příkazu **REFRESH SECURITY** , který je nezbytný k aktivaci profilů.

Nastavení zabezpečení produktu IBM MQ MQI client

Je třeba zvážit zabezpečení produktu IBM MQ MQI client , aby klientské aplikace neměly neomezený přístup k prostředkům na serveru.

Když spouštíte aplikaci klienta, nespouštějte aplikaci pomocí ID uživatele, které má více přístupových práv, než je nezbytné, například uživatel ve skupině `mqm` nebo dokonce sám uživatel `mqm` .

Spustíte-li aplikaci jako uživatele s příliš mnoha přístupovými právy, riskujete přístup k aplikaci a změnou částí správce front, a to buď omylem, nebo neúmyslně.

Mezi aplikací klienta a jeho serverem správce front existují dva aspekty zabezpečení: ověřování a řízení přístupu.

- Ověřování lze použít k ujištění, že klientská aplikace spuštěná jako specifický uživatel je tím, kým říkají, že jsou. Použitím ověření můžete zabránit útočníkovi získat přístup k vašemu správci front tím, že zosobňujete jednu z vašich aplikací.

  V produktu IBM MQ 8.0je ověření poskytnuto jednou ze dvou možností:

  – Funkce ověření připojení.

    Další informace o ověření připojení viz “Ověření připojení” na stránce 66.

  – Použití vzájemného ověření v rámci TLS.

    Další informace o protokolu TLS najdete v tématu “Práce s protokolem SSL” na stránce 268.

- Řízení přístupu lze použít k udělení nebo odebrání přístupových práv pro určitého uživatele nebo skupinu uživatelů. Spuštěním klientské aplikace se specificky vytvořeným uživatelem (nebo uživatelem ve specifické skupině) můžete pomocí ovládacích prvků přístupu zajistit, že aplikace nebude mít přístup k částem správce front, o které nemá aplikace pracovat.

  Při nastavení řízení přístupu je třeba zvážit pravidla ověřování kanálu a pole MCAUSER na kanálu. Obě tyto funkce mají schopnost změnit, které ID uživatele se používá pro ověření práv k řízení přístupu.

  Další informace o řízení přístupu viz “Autorizace přístupu k objektům” na stránce 342.

Pokud jste nastavili klientskou aplikaci pro připojení ke specifickému kanálu s omezeným ID, ale kanál má nastaveno ID administrátora v poli MCAUSER, pak za předpokladu, že se klientská aplikace úspěšně

připojí, použije se ID administrátora pro kontroly řízení přístupu. Klientská aplikace proto bude mít úplná přístupová práva k vašemu správci front.

Další informace o atributu MCAUSER viz “Mapování ID uživatele klienta na ID uživatele MCAUSER” na stránce 377.

Pravidla ověřování kanálu lze také použít jako metodu pro řízení přístupu ke správci front, nastavením specifických pravidel a kritérií pro připojení, které má být přijato.

Další informace o pravidlech ověřování kanálu viz: “Záznamy ověření kanálu” na stránce 47.

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" . Certifikát pro tento modul byl přesunut do historického stavu. Zákazníci by si měli prohlédnout IBM Crypto for C certificate a měli by si být vědomi jakýchkoli 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 konfiguračním souboru klienta na hodnotu YES.

Standardně se specifikace CipherSpecs s certifikací FIPS nepožadují.

Tyto hodnoty mají stejný význam jako ekvivalentní hodnoty parametrů v příkazu ALTER QMGR SSLFIPS (viz ALTER QMGR). 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.

Je-li konfigurován pouze standard FIPS CipherSpecs , klient MQI odmítne připojení, která neurčují specifikaci CipherSpec standardu FIPS s hodnotou 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 32
Je-li na kanálu SSL/TLS v systémech AIX, Linux, and Windows vyžadováno šifrování, produkt IBM MQ používá 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.

Související odkazy

FipsRequired (MQLONG)
MQSSLFIPS

Sekce SSL konfiguračního souboru klienta

AIX Spuštění klientských aplikací TLS s více instalacemi sady GSKit V8.0 v systému AIX

Aplikace klienta TLS v produktu AIX mohou zaznamenat MQRC_CHANNEL_CONFIG_ERROR a chybu AMQ6175 , pokud jsou spuštěny na systémech AIX s více instalacemi sady GSKit V8.0 .

Při spouštění klientských aplikací v systému AIX s více instalacemi sady GSKit V8.0 může volání spojení klienta vrátit produkt MQRC_CHANNEL_CONFIG_ERROR při použití TLS. Protokol /var/mqm/errors zaznamenává chybu záznamu 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 to, že nastavení proměnné prostředí LIBPATH nebo LD_LIBRARY_PATH způsobilo, že klient produktu IBM MQ zaváděl smíšenou sadu knihoven ze dvou různých instalací sady GSKit V8.0 . Tato chyba může způsobit provedení klientské aplikace IBM MQ v prostředí produktu Db2 .

Chcete-li se této chybě vyhnout, zahrňte do cesty ke knihovně adresáře knihovny IBM MQ , aby měly knihovny IBM MQ přednost. Toho lze dosáhnout pomocí příkazu **setmqenv** s parametrem **-k** , například:

```
. /usr/mqm/bin/setmqenv -s -k
```

Další informace o použití příkazu **setmqenv** naleznete v části setmqenv (nastavení prostředí IBM MQ)

IBM i Nastavení komunikace pro SSL nebo TLS v systému IBM i

Zabezpečené komunikace, které používají šifrovací bezpečnostní protokoly SSL nebo TLS, zahrnují nastavení komunikačních kanálů a správu digitálních certifikátů, které budete používat pro ověření.

Chcete-li nastavit zabezpečení SSL nebo TLS, je třeba definovat kanály pro použití zabezpečení SSL nebo TLS. Musíte také vytvořit a spravovat digitální certifikáty. V některých operačních systémech můžete provádět testy s certifikáty s vlastním podpisem. V systému IBM ivšak musíte používat osobní certifikáty podepsané lokálním CA.

Chcete-li získat úplné informace o vytváření a správě certifikátů, prohlédněte si téma “Práce s SSL/TLS v IBM i” na stránce 268.

Tato kolekce témat představuje některé z úloh souvisejících s nastavením komunikace SSL nebo TLS a poskytuje pokyny k provedení těchto úloh podle kroku.

Možná budete chtít testovat také ověření klienta SSL nebo TLS, které jsou volitelné části protokolů SSL a TLS. Při navázání komunikace přes zabezpečení SSL nebo TLS vždy klient SSL nebo TLS získává a ověřuje digitální certifikát ze serveru. Při použití implementace produktu IBM MQ server SSL nebo TLS vždy požaduje certifikát od klienta.

V systému IBM iodešle klient SSL nebo TLS certifikát pouze v případě, že má jeden 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`.
- Pro klienta IBM MQ C for IBM i, `ibmwebspheremq` následovalo vaše přihlašovací ID uživatele se změnil na malá písmena, například `ibmwebspheremqmyuserid`.

IBM MQ používá předponu `ibmwebspheremq` na štítku, aby nedošlo k záměně s certifikáty pro jiné produkty. Ujistěte se, že jste zadali celé návěští certifikátu malými písmeny.

Server SSL nebo TLS vždy ověřuje platnost certifikátu klienta, je-li odeslán. Pokud klient SSL nebo TLS neodešle certifikát, ověření selže pouze tehdy, když je konec kanálu, který funguje jako server SSL nebo TLS, definován buď s parametrem SSLCAUTH nastaveným na hodnotu REQUIRED nebo nastaveným na hodnotu parametru SSLPEER. Další informace naleznete v tématu Připojení dvou správců front s použitím zabezpečení SSL nebo TLS.

ALW Nastavení komunikace pro SSL nebo TLS v systému AIX, Linux, and Windows

Zabezpečené komunikace, které používají šifrovací bezpečnostní protokoly SSL nebo TLS, zahrnují nastavení komunikačních kanálů a správu digitálních certifikátů, které budete používat pro ověření.

Chcete-li nastavit zabezpečení SSL nebo TLS, je třeba definovat kanály pro použití zabezpečení SSL nebo TLS. Musíte také vytvořit a spravovat digitální certifikáty. V systému AIX, Linux, and Windows můžete provádět testy s certifikáty s vlastním podpisem.

Upozornění: Není možné použít směs certifikátů podepsaných Elliptic Curve a RSA podepsaných pro správce front, které chcete spojit pomocí kanálů s povoleným zabezpečením TLS.

Správci front používající kanály s povoleným zabezpečením TLS musí všechny používat certifikáty podepsané RSA nebo všechny certifikáty podepsané EC, nikoli směs obou těchto certifikátů.

Další informace viz “Digitální certifikáty a kompatibilita CipherSpec v produktu IBM MQ” na stránce 43.

Certifikáty podepsané sebou samým nelze odvolat, což by mohlo útočníkovi umožnit, aby se identita po soukromém klíči zkompromitovala. Certifikační úřady mohou odvolat kompromitovaný certifikát, který zabrání jeho dalšímu použití. Certifikáty podepsané certifikační autoritou jsou proto bezpečnější pro použití v produkčním prostředí, ačkoli certifikáty podepsané sebou samým pro testovací systém jsou pohodlnější.

Chcete-li získat úplné informace o vytváření a správě certifikátů, prohlédněte si téma “Práce s SSL/TLS v AIX, Linux, and Windows” na stránce 279.

Tato kolekce témat představuje některé z úloh souvisejících s nastavením komunikace SSL a poskytuje pokyny k provedení těchto úloh podle kroku.

Možná budete chtít testovat také ověření klienta SSL nebo TLS, které jsou volitelnou částí protokolů. Při navázání komunikace přes zabezpečení SSL nebo TLS vždy klient SSL nebo TLS získává a ověřuje digitální certifikát ze serveru. Při použití implementace produktu IBM MQ server SSL nebo TLS vždy požaduje certifikát od klienta.

V systému AIX, Linux, and Windowsodešle klient SSL nebo TLS certifikát pouze v případě, že má jeden popisek ve správném formátu IBM MQ :

- V případě správce front je formát `ibmwebspheremq` následován názvem správce front, který byl změněn na malá písmena. Například pro `QM1`, `ibmwebspheremqqm1`
- V případě klienta IBM MQ je `ibmwebspheremq` následováno vaším přihlašovacím ID uživatele změněno na malá písmena, například `ibmwebspheremqmyuserid`.

IBM MQ používá předponu `ibmwebspheremq` na štítku, aby nedošlo k záměně s certifikáty pro jiné produkty. Ujistěte se, že jste zadali celé návěští certifikátu malými písmeny.

Server SSL nebo TLS vždy ověřuje platnost certifikátu klienta, je-li odeslán. Pokud klient neodešle certifikát, ověření selže pouze tehdy, když je konec kanálu, který funguje jako server SSL nebo TLS, definován buď s parametrem SSLCAUTH nastaveným na hodnotu REQUIRED nebo s nastavenou hodnotou parametru SSLPEER. Další informace naleznete v tématu Připojení dvou správců front s použitím 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 s SSL/TLS v z/OS” na stránce 310.

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 protokolem SSL

Tato témata uvádějí pokyny pro provádění jednotlivých úloh souvisejících s použitím TLS s produktem IBM MQ.

Mnoho z nich se používá jako kroky v úlohách vysoké úrovně popsaných v následujících sekcích:

- “Identifikace a ověřování uživatelů” na stránce 322
- “Autorizace přístupu k objektům” na stránce 342
- “Důvěrnost zpráv” na stránce 408
- “Integrita dat zpráv” na stránce 465
- “Uchování zabezpečených klastrů” na stránce 466

IBM i Práce s SSL/TLS v IBM i

Tato kolekce témat obsahuje pokyny pro jednotlivé úlohy pracující s protokolem TLS (Transport Layer Security) v produktu IBM MQ for IBM i.

Pro IBM i je podpora TLS nedílnou součástí operačního systému. Ujistěte se, že jste nainstalovali nezbytné předpoklady uvedené v tématu Hardwarové a softwarové požadavky na produktu IBM i.

V systému IBM ispravujete klíče a digitální certifikáty pomocí nástroje Digital Certificate Manager (DCM).

Přístup k DCM

Postupujte podle těchto pokynů pro přístup k rozhraní DCM.

Informace o této úloze

Proveďte následující kroky ve webovém prohlížeči, který podporuje rámce.

Postup

1. Přejděte do adresáře `http://`*`machine`*`.domain:2001` nebo `https://`*`machine`*`.domain:2010`, kde *machine* je název vašeho počítače.
2. Zadejte platný uživatelský profil a heslo, je-li to požadováno.

   Ujistěte se, že váš uživatelský profil má speciální oprávnění *ALLOBJ a *SECADM, abyste mohli vytvářet nová úložiště certifikátů. Nemáte-li speciální oprávnění, můžete spravovat pouze své osobní certifikáty nebo zobrazit podpisy objektů pro objekty, pro které máte oprávnění. Máte-li oprávnění k použití aplikace pro podepisování objektů, můžete také podepisovat objekty z DCM.
3. Na stránce Konfigurace Internetu klepněte na **Digital Certificate Manager**.

   Zobrazí se stránka Digitální Certificate Manager .

Přiřazení certifikátu ke správci front v systému IBM i

Použijte produkt DCM k přiřazení certifikátu ke správci front.

K přiřazení certifikátu ke správci front použijte tradiční správu digitálních certifikátů produktu IBM i . To znamená, že můžete uvést, že správce front používá systémové úložiště certifikátů a že je správce front

registrován pro použití jako aplikace s DCM (Digital Certificate Manager. Chcete-li to provést, změňte hodnotu atributu **SSLKEYR** správce front na *SYSTEM.

Je-li parametr **SSLKEYR** změněn na *SYSTEM, produkt IBM MQ registruje správce front jako serverovou aplikaci s jedinečným popiskem aplikace fronty QIBM_WEBSPHERE_MQ_QMGRNAME a štítkem s popisem Qmgrname (WMQ). Všimněte si, že atributy kanálu **CERTLABL** se nepoužijí, používáte-li paměť certifikátů *SYSTEM. Správce front se poté zobrazí jako serverová aplikace v produktu Digital Certificate Managera můžete této aplikaci přiřadit libovolný serverový nebo klientský certifikát v systémovém úložišti.

Vzhledem k tomu, že správce front je registrován jako aplikace, lze provádět rozšířené funkce produktu DCM, jako je například definování důvěryhodných seznamů CA.

Pokud se parametr **SSLKEYR** změní na jinou hodnotu než *SYSTEM, IBM MQ zruší registraci správce front jako aplikaci s DCM (Digital Certificate Manager. Je-li správce front odstraněn, je také z DCM deregistrován. Uživatel s dostatečným oprávněním *SECADM může také ručně přidávat nebo odebírat aplikace z DCM.

Nastavení úložiště klíčů v systému IBM i

Na obou koncích připojení musí být nastaveno úložiště klíčů. Lze použít výchozí úložiště certifikátů, nebo můžete vytvořit vlastní úložiště certifikátů.

Připojení TLS vyžaduje *úložiště klíčů* na každém konci připojení. Každý správce front a produkt IBM MQ MQI client musí mít přístup k úložišti klíčů. Chcete-li přistoupit k úložišti klíčů pomocí názvu souboru a hesla (tj. ne pomocí volby *SYSTEM), ujistěte se, že uživatelský profil QMQM má následující oprávnění:

- Oprávnění k provedení pro adresář obsahující úložiště klíčů
- Oprávnění ke čtení pro soubor obsahující úložiště klíčů

Další informace viz “Úložiště klíčů SSL/TLS” na stránce 23. Všimněte si, že atributy kanálu **CERTLABL** se nepoužijí, používáte-li paměť certifikátů *SYSTEM.

V systému IBM ijsou digitální certifikáty uloženy v úložišti certifikátů, které je spravováno produktem DCM. Tyto digitální certifikáty mají štítky, které přidružují certifikát ke správci front nebo k produktu IBM MQ MQI client. TLS používá certifikáty pro účely autentizace.

Jmenovka je buď hodnota atributu **CERTLABL** , je-li nastavena, nebo standardní `ibmwebspheremq` s připojeným jménem správce front nebo přihlašovacího ID uživatele IBM MQ MQI client , vše malými písmeny. Podrobnosti najdete v tématu Digitální certifikáty certifikátu .

Název správce front nebo úložiště certifikátů produktu IBM MQ MQI client se skládá z cesty a názvu kmene. Výchozí cesta je `/QIBM/UserData/ICSS/Cert/Server/` a výchozí název kmene je `Default`. V produktu IBM ije výchozí úložiště certifikátů, `/QIBM/UserData/ICSS/Cert/Server/Default.kdb`, také známé jako *SYSTEM. Volitelně můžete definovat vlastní cestu a název kmene.

Definujete-li vlastní cestu nebo název souboru, nastavte oprávnění k souboru tak, aby k němu měl přístup těsně pod kontrolou.

Příkaz “Změna umístění úložiště klíčů pro správce front v systému IBM i” na stránce 271 vám sděluje informace o určení názvu úložiště certifikátů. Název úložiště certifikátů můžete zadat buď před vytvořením úložiště certifikátů, nebo po něm.

Poznámka: Operace, které můžete provádět s DCM, mohou být omezeny oprávněním vašeho uživatelského profilu. Například vyžadujete oprávnění *ALLOBJ a *SECADM pro vytvoření certifikátu CA.

Vytvoření úložiště certifikátů v systému IBM i

Pokud nechcete použít výchozí úložiště certifikátů, postupujte podle této procedury a vytvořte vlastní úložiště certifikátů.

Informace o této úloze

Vytvořte nové úložiště certifikátů pouze v případě, že nechcete používat výchozí úložiště certifikátů produktu IBM i .

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

Postup

1. Přistupte k rozhraní DCM, jak je popsáno v “Přístup k DCM” na stránce 268
2. V navigačním panelu klepněte na volbu **Vytvořit nové úložiště certifikátů**.
   V rámci úlohy se zobrazí stránka Vytvoření nové paměti certifikátů.
3. V rámci úlohy vyberte volbu **Jiná systémová paměť certifikátů** a klepněte na tlačítko **Pokračovat**.
   V rámci úlohy se zobrazí stránka Vytvoření certifikátu v nové paměti certifikátů.
4. Vyberte volbu **Ne-Nevytvářet certifikát v úložišti certifikátů** a klepněte na tlačítko **Pokračovat**.
   V rámci úlohy se zobrazí stránka Název úložiště certifikátů a heslo.
5. Do pole **Cesta k úložišti certifikátů a název souboru** zadejte cestu k souboru IFS a název souboru, například `/QIBM/UserData/mqm/qmgrs/qm1/key.kdb`
6. Do pole **Heslo** zadejte heslo a zadejte je znovu do pole **Potvrdit heslo** . Klepněte na tlačítko **Pokračovat**.
   Poznamenejte si heslo (je citlivé na velikost písmen), protože jej budete potřebovat při ukládání klíče úložiště.
7. Chcete-li ukončit práci s produktem DCM, zavřete okno prohlížeče.

Jak pokračovat dále

Když jste vytvořili paměť certifikátů pomocí produktu DCM, ujistěte se, že jste heslo uložili, jak je popsáno v “Uložení hesla k úložišti certifikátů v systémech IBM i” na stránce 270

Související úlohy

“Import certifikátu do úložiště klíčů v systému IBM i” na stránce 275
Chcete-li importovat certifikát, postupujte podle této procedury.

Uložení hesla k úložišti certifikátů v systémech IBM i

Založit heslo k úložišti certifikátů pomocí CL příkazů.

Následující pokyny se vztahují na ukládání hesla úložiště certifikátů v systému IBM i pro správce front. Alternatively, for an IBM MQ MQI client, if you are not using the *SYSTEM certificate store (that is, the MQSSLKEYR environment is set to a value other than *SYSTEM), follow the procedure described in the “Uskladovat heslo k úložišti certifikátů” na stránce 278 section of “Obslužný program IBM MQ SSL Client (amqrsslc) pro IBM i” na stránce 277.

Jestliže jste uvedli, že paměť certifikátů *SYSTEM má být použita (změnou hodnoty atributu SSLKEYR ze správce front na *SYSTEM), nesmíte tyto kroky provést.

Když jste pomocí produktu DCM vytvořili úložiště certifikátů, použijte následující příkazy k uložení hesla:

```
STRMQM MQMNAME('queue_manager_name')
CHGMQM MQMNAME('queue_manager_name') SSLKEYRPWD('password')
```

V heslu se rozlišují malá a velká písmena. Musí být zadán v jednoduchých uvozovkách přesně tak, jak jste jej zadali v kroku 6 dokumentu “Vytvoření úložiště certifikátů v systému IBM i” na stránce 269.

Poznámka: Pokud nepoužíváte výchozí systémové úložiště certifikátů a neuložíte heslo, pokusy o spuštění kanálů TLS selžou, protože nemohou získat heslo potřebné pro přístup k paměti certifikátů.

Vyhledání úložiště klíčů pro správce front v systému IBM i

Tento postup slouží k získání umístění úložiště certifikátů správce front.

Postup

1. Zobrazte atributy správce front pomocí následujícího příkazu:

```
DSPMQM MQMNAME('queue manager name')
```

2. Prověřte 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

Pro nastavení atributu úložiště klíčů správce front použijte buď příkaz CHGMQM, nebo příkaz ALTER QMGR MQSC.

a) Použití CHGMQM: `CHGMQM MQMNAME('qm1') SSLKEYR('/QIBM/UserData/ICSS/Cert/Server/MyKey')`

b) Použití příkazu ALTER QMGR: `ALTER QMGR SSLKEYR('/QIBM/UserData/ICSS/Cert/Server/MyKey')`

V obou případech má úložiště certifikátů plně kvalifikovaný název souboru: `/QIBM/UserData/ICSS/Cert/Server/MyKey.kdb`

Jak pokračovat dále

Změníte-li umístění úložiště certifikátů správce front, nebudou certifikáty přeneseny ze starého umístění. Pokud jsou certifikáty CA předinstalované při vytváření úložiště certifikátů nedostatečné, je třeba naplnit nové úložiště certifikátů certifikáty, jak je popsáno v tématu “Import certifikátu do úložiště klíčů v systému IBM i” na stránce 275. Musíte také odložit heslo pro nové umístění, jak je popsáno v tématu “Uložení hesla k úložišti certifikátů v systémech IBM i” na stránce 270.

Vytvoření certifikační autority a certifikátu pro testování v systému IBM i

Tento postup slouží k vytvoření certifikátu lokálního CA pro podepisování požadavků na certifikát 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 na “Požádání o certifikát serveru v systému IBM i” na stránce 272.

Informace o této úloze

Certifikáty CA, které jsou poskytovány při instalaci TLS, jsou podepsány vydavatelem CA. V systému IBM imůžete generovat lokální certifikační autoritu, která může podepisovat certifikáty serveru pro účely testování komunikace TLS ve vašem systému. Chcete-li vytvořit lokální certifikát CA, postupujte takto ve webovém prohlížeči:

Postup

1. Přistupte k rozhraní DCM, jak je popsáno v tématu “Přístup k DCM” na stránce 268.
2. V navigačním panelu klepněte na volbu **Vytvořit certifikační autoritu**.

   V rámci úlohy se zobrazí stránka Vytvoření certifikační autority.
3. Do pole **Heslo úložiště certifikátů** zadejte heslo a zadejte jej znovu do pole **Potvrdit heslo** .
4. Zadejte název do pole **Název vydavatele certifikátů (CA)** , například `TLS Test Certificate Authority`.
5. Zadejte příslušné 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 lokálního CA.

   Výchozí hodnota je 1095 dnů.

7. Klepněte na tlačítko **Pokračovat**.
   Vytvoří se CA a DCM vytvoří paměť certifikátů a certifikát CA pro vašeho lokálního CA.
8. Klepněte na tlačítko **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. Jakmile je stahování dokončeno, klepněte na tlačítko **Otevřít**.
    Zobrazí se okno certifikátu.
11. Klepněte na tlačítko **Instalovat certifikát**.
    Zobrazí se průvodce importem certifikátu.
12. Klepněte na tlačítko **Další**.
13. Vyberte volbu **Automaticky vybrat paměť 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**.
    Stránka Zásada certifikační autority se zobrazí v rámci úlohy.
18. V poli **Povolit vytvoření uživatelských certifikátů** vyberte volbu **Ano**.
19. Do pole **Období platnosti** zadejte období platnosti certifikátů, které jsou vydány vaším lokálním CA.
    Výchozí hodnota je 365 dní.
20. Klepněte na tlačítko **Pokračovat**.
    V rámci úlohy se zobrazí stránka Vytvoření certifikátu v nové paměti certifikátů.
21. Zkontrolujte, zda není vybrána žádná z aplikací.
22. Chcete-li dokončit nastavení lokálního CA, klepněte na **Pokračovat** .

Požádání o certifikát serveru v systému IBM i

Digitální certifikáty chrání před ztělesněním a potvrzují, že veřejný klíč patří do zadané entity. Certifikát nového serveru lze požadovat od vydavatele certifikátů 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 DCM” na stránce 268.
2. V navigačním panelu klepněte na **Výběr úložiště certifikátů**.
   V rámci úlohy se zobrazí stránka Výběr úložiště certifikátů.
3. Vyberte úložiště certifikátů, které chcete použít, a klepněte na **Pokračovat**.
4. Volitelné: Pokud jste v kroku 3 vybrali ***SYSTEM** , zadejte heslo do systémového úložiště a klepněte na **Pokračovat**.
5. Volitelné: Pokud jste v kroku 3 vybrali volbu **Jiná systémová paměť certifikátů** , v poli **Cesta k úložišti certifikátů a název souboru** zadejte cestu k souboru IFS a název souboru, který jste nastavili při vytváření paměti certifikátů. Do pole **Heslo úložiště certifikátů** zadejte také heslo. Pak klepněte na **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 Select a Certificate Authority (CA).

8. Máte-li na pracovní stanici lokálního CA, zvolte buď lokální CA, nebo komerční CA k podepsání certifikátu. Vyberte přepínač pro CA, který chcete, a klepněte na **Pokračovat**.

   V rámci úlohy se zobrazí stránka Vytvoření certifikátu.

9. Volitelné: V případě správce front zadejte do pole **Popisek certifikátu** jmenovku certifikátu.

   Jmenovka je buď hodnota atributu **CERTLABL** , pokud je nastavena, nebo standardní `ibmwebspheremq` s připojeným názvem správce front, vše malými písmeny. Podrobnosti najdete v tématu Digitální certifikáty certifikátu .

   Například pro správce front QM1zadejte `ibmwebspheremqqm1` pro použití výchozí hodnoty.

10. Volitelné: Pro IBM MQ MQI clientv poli **Označení certifikátu** zadejte `ibmwebspheremq` následované ID uživatele pro přihlášení složené na malá písmena.
    Zadejte například `ibmwebspheremqmyuserID`
11. Zadejte příslušné hodnoty do polí **Obecný název** a **Organizace** a vyberte zemi. Pro zbývající volitelná pole zadejte požadované hodnoty.

Výsledky

Pokud jste vybrali komerční CA k podepsání vašeho certifikátu, produkt DCM vytvoří žádost o certifikát ve formátu PEM (Privacy-Enhanced Mail). Postoupit požadavek na zvolenou CA.

Pokud jste vybrali lokálního CA pro podepsání vašeho certifikátu, produkt DCM vás informuje o tom, že certifikát byl vytvořen v paměti certifikátů a lze jej použít.

Požádání o certifikát serveru pro produkt IBM Key Manager na systému IBM i

Postupujte takto, chcete-li vytvořit certifikát podepsaný vaší lokální certifikační autoritou (CA) nebo požádat o certifikát serveru podepsaný komerční CA pro import do obslužného programuiKeyman(Správa klíčů produktu IBM).

Informace o této úloze

Certifikát uživatele musí být použit, když DCM (Digital Certificate Manager) slouží jako správce certifikátů pro IBM MQ na více platformách. V případě osobních certifikátů distribuovaných na jiných platformách 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 DCM” na stránce 268.
2. V podokně **navigace** klepněte na volbu **Vytvořit certifikát**.

   Stránka **Vytvořit certifikát** se zobrazí v rámci úlohy.

3. Na panelu **Vytvořit certifikát** vyberte přepínač **Certifikát uživatele** a klepněte na tlačítko **Pokračovat**.

   Zobrazí se stránka **Vytvoření uživatelského certifikátu** .

4. Na panelu **Vytvořit uživatelský certifikát** vyplňte povinná pole pod informacemi o certifikátu pro **Název organizace**, **Stav** nebo **kraj**, **Země** nebo **region**. Volitelně zadejte hodnoty do polí **Organizační jednotka** a **Lokalita** nebo **Město** . Klepněte na tlačítko **Pokračovat**.

   Obecný název je automaticky nastaven na ID uživatele, se kterým jste přihlášeni do systému iSeries .

5. Na dalším panelu **Vytvořit uživatelský certifikát** klepněte na **Instalovat certifikát** a klepněte na **Pokračovat**.

   Zobrazí se zpráva s textem `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 DCM, proveďte následující kroky:
   a) Pro volbu Microsoft Edge vyberte: **Nástroje > Možnosti Internetu > karta Obsah > Tlačítko Certifikáty > Osobní karta >**. Vyberte certifikát a klepněte na tlačítko **Exportovat**.

b) Pro prohlížeč Mozilla Firefox vyberte volbu **Tools> Options > Advanced> Encryption tab > View Certificates button > Your Certificates tab >**. Vyberte certifikát a klepněte na tlačítko **Zálohovat**. Vyberte cestu a název souboru a klepněte na tlačítko **OK**.

8. Přeneste exportovaný certifikát do vzdáleného systému 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 uvedených v tématu Import ze souboru Microsoft `.pfx` .
   b) Pokud byl certifikát uložen pomocí prohlížeče Mozilla Firefox, postupujte podle pokynů uvedených v tématu Import osobního certifikátu do úložiště klíčů.

   Během importu zkontrolujte, zda se název štítku osobního certifikátu a certifikát podepsaného mění na to, co očekává IBM MQ . Návěští musí být buď hodnota atributu IBM MQ **CERTLABL** , je-li nastavena, nebo standardní `ibmwebspheremq` s připojeným názvem správce front, vše malými písmeny. Podrobnosti najdete v tématu Digitální certifikáty certifikátu .

Přidání certifikátů serveru do úložiště klíčů v systému IBM i

Postupujte podle této procedury a přidejte požadovaný certifikát do úložiště klíčů.

Informace o této úloze

Poté, co certifikační autorita odešle nový certifikát serveru, jej přidáte do úložiště certifikátů, ze kterého jste požadavek vygenerovali. Pokud CA odešle certifikát jako část e-mailové zprávy, zkopírujte tento certifikát do samostatného souboru.

Poznámka:

- Tuto proceduru nemusíte provádět, pokud je certifikát serveru podepsán vaším lokálním CA.
- Dříve než importujete certifikát serveru ve formátu PKCS #12 do 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 DCM” na stránce 268.
2. V kategorii úloh **Spravovat certifikáty** v navigačním panelu klepněte na volbu **Importovat certifikát**.

   Stránka Importovat certifikát se zobrazí v rámci úlohy.
3. Vyberte přepínač pro daný typ certifikátu a klepněte na tlačítko **Pokračovat**.

   V rámci úlohy se zobrazí buď stránka Import serveru, Certifikát klienta, nebo stránka Import certifikátu certifikační autority (CA).
4. V poli **Importovat soubor** zadejte název souboru certifikátu, který chcete importovat, a klepněte na **Pokračovat**.

   Produkt DCM automaticky určí formát souboru.
5. Je-li certifikátem certifikát **Server nebo klient** , zadejte heslo do rámce úloh a klepněte na tlačítko **Pokračovat**.

   Produkt DCM vás informuje o tom, že certifikát byl importován.

Export certifikátu z úložiště klíčů v systému IBM i

Export certifikátu exportuje jak veřejný, tak soukromý klíč. Tato akce by měla být přijímána s extrémní opatrností, protože předání na soukromý klíč by zcela ohrozilo vaši bezpečnost.

Než začnete

Sdílíte-li uživatelský certifikát s jiným uživatelem, vyměňujete veřejné klíče. Tento proces je popsán v tématu **Úloha 5. Sdílení certifikátů** v sekci Sdílení certifikátů produktu “Stručná úvodní příručka pro AMS v systému AIX and Linux” na stránce 596. Když exportujete certifikát, jak je popsáno zde, exportujete

veřejný i soukromý klíč. Tato akce by měla být přijímána s extrémní opatrností, protože předání na soukromý klíč by zcela ohrozilo vaši bezpečnost.

Informace o této úloze

Na počítači, ze kterého chcete exportovat certifikát, proveďte následující kroky:

Postup

1. Přistupte k rozhraní DCM, jak je popsáno v tématu “Přístup k DCM” na stránce 268.
2. V navigačním panelu klepněte na **Výběr úložiště certifikátů**.
   V rámci úlohy se zobrazí stránka Výběr úložiště certifikátů.
3. Vyberte úložiště certifikátů, které chcete použít, a klepněte na **Pokračovat**.
4. Volitelné: Pokud jste v kroku 3 vybrali ***SYSTEM** , zadejte heslo do systémového úložiště a klepněte na **Pokračovat**.
5. Volitelné: Pokud jste v kroku 3 vybrali volbu **Jiná systémová paměť certifikátů** , v poli **Cesta a název souboru úložiště certifikátů** zadejte cestu k souboru IFS a název souboru, který jste nastavili při vytváření paměti certifikátů, a zadejte heslo do pole **Heslo úložiště certifikátů** . Pak klepněte na **Pokračovat**
6. V kategorii úloh **Spravovat certifikáty** v navigačním panelu klepněte na volbu **Exportovat certifikát**.
   Stránka Export certifikátu se zobrazí v rámci úlohy.
7. Vyberte přepínač pro daný typ certifikátu a klepněte na tlačítko **Pokračovat**.
   V rámci úlohy se zobrazí buď stránka Export Server, nebo stránka certifikátu klienta, nebo stránka certifikátu exportu certifikační autority (CA).
8. Vyberte certifikát, který chcete exportovat.
9. Vyberte přepínač, abyste uvedli, zda chcete exportovat certifikát do souboru nebo přímo do jiného úložiště certifikátů.
10. Pokud jste vybrali exportování certifikátu serveru nebo klienta do souboru, zadejte následující informace:
    - Cesta a název souboru umístění, do kterého chcete uložit exportovaný certifikát.
    - Pro osobní certifikát se jedná o heslo, které se používá k zašifrování exportovaného certifikátu a vydání na cílovém systému. Pro certifikáty CA není třeba zadávat heslo.
11. Pokud jste vybrali export certifikátu přímo do jiného úložiště certifikátů, určete 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

Než naimportujete osobní certifikát ve formátu PKCS #12 do DCM, musíte nejprve importovat odpovídající certifikát CA.

Informace o této úloze

Proveďte tyto kroky na počítači, na který chcete importovat certifikát.

Postup

1. Přistupte k rozhraní DCM, jak je popsáno v tématu “Přístup k DCM” na stránce 268.
2. V navigačním panelu klepněte na **Výběr úložiště certifikátů**.
   V rámci úlohy se zobrazí stránka Výběr úložiště certifikátů.
3. Vyberte úložiště certifikátů, které chcete použít, a klepněte na **Pokračovat**.

4. Volitelné: Pokud jste v kroku 3 vybrali ***SYSTEM** , zadejte heslo do systémového úložiště a klepněte na **Pokračovat**.
5. Volitelné: Pokud jste v kroku 3 vybrali volbu **Jiná systémová paměť certifikátů** , v poli **Cesta a název souboru úložiště certifikátů** zadejte cestu k souboru IFS a název souboru, který jste nastavili při vytváření paměti certifikátů, a zadejte heslo do pole **Heslo úložiště certifikátů** . Pak klepněte na **Pokračovat**
6. V kategorii úloh **Spravovat certifikáty** v navigačním panelu klepněte na volbu **Importovat certifikát**.

   Stránka Importovat certifikát se zobrazí v rámci úlohy.
7. Vyberte přepínač pro daný typ certifikátu a klepněte na tlačítko **Pokračovat**.

   V rámci úlohy se zobrazí buď stránka Import serveru, Certifikát klienta, nebo stránka Import certifikátu certifikační autority (CA).
8. V poli **Importovat soubor** zadejte název souboru certifikátu, který chcete importovat, a klepněte na **Pokračovat**.

   Produkt DCM automaticky určí formát souboru.
9. Je-li certifikátem certifikát **Server nebo klient** , zadejte heslo do rámce úloh a klepněte na tlačítko **Pokračovat**. Produkt DCM vás informuje o tom, že certifikát byl importován.

Odebrání certifikátů v produktu IBM i

Tento postup slouží k odebrání osobních certifikátů.

Postup

1. Přistupte k rozhraní DCM, jak je popsáno v tématu “Přístup k DCM” na stránce 268.
2. V navigačním panelu klepněte na **Výběr úložiště certifikátů**.

   V rámci úlohy se zobrazí stránka Výběr úložiště certifikátů.
3. Označte zaškrtávací políčko **Další systémové úložiště certifikátů** a klepněte na **Pokračovat**.

   Zobrazí se stránka Paměť certifikátů a heslo.
4. Do pole **Cesta k úložišti certifikátů a název souboru** zadejte cestu k souboru IFS a název souboru, který jste nastavili při vytváření paměti certifikátů.
5. Do pole **Heslo úložiště certifikátů** zadejte heslo. Klepněte na tlačítko **Pokračovat**.

   V rámci úlohy se zobrazí stránka Aktuální úložiště certifikátů.
6. V kategorii úloh **Správa certifikátů** v navigačním panelu klepněte na volbu **Odstranit certifikát**.

   V rámci úlohy se zobrazí stránka Potvrzení 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 o tom, že certifikát odstranil.

*Použití úložiště certifikátů *SYSTEM pro jednosměrné ověření v systému IBM i*

Postupujte podle těchto pokynů, chcete-li nastavit jednosměrné ověření.

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 naimportuje jej do úložiště klíčů.
- Spusťte modul listener na správci front serveru a klienta.

Informace o této úloze

Chcete-li použít jednosměrnou autentizaci, použijte počítač se serverem IBM i jako server TLS, nastavte parametr SSLKEYR (Secure Key Repository) na *SYSTEM. Toto nastavení registruje správce front produktu IBM MQ jako aplikaci. Poté můžete přiřadit certifikát správci front, který povolí jednosměrné ověření.

Soukromá úložiště klíčů můžete také použít k implementaci jednosměrného ověření vytvořením fiktivního certifikátu pro správce front klienta v úložišti klíčů.

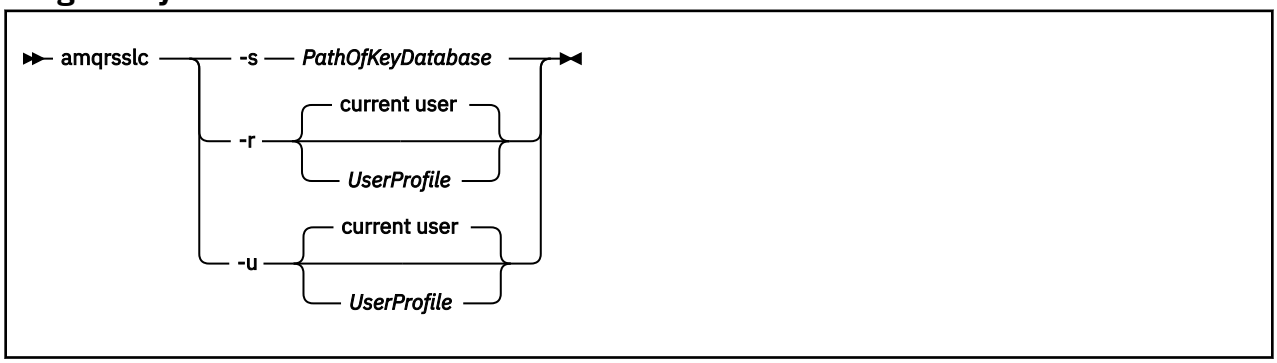
Postup

1. Na serveru a ve správcích front klienta proveďte následující kroky:
   a) Upravte správce front tak, aby nastavil parametr SSLKEYR zadáním příkazu `CHGMQM MQMNAME(SSL) SSLKEYR(*SYSTEM)`.
   b) Založit heslo pro výchozí úložiště klíčů zadáním příkazu `CHGMQM MQMNAME(SSL) SSLKEYRPWD('xxxxxxx')`.
      Heslo musí být v jednoduchých uvozovkách.
   c) Upravte kanály tak, aby měly v parametru SSLCIPHERE správnou položku CipherSpec .
   d) Aktualizujte zabezpečení TLS zadáním příkazu `RFRMQMAUT QMNAME(QMGRNAME) TYPE(*SSL)`.
2. Přiřaďte certifikát ke správci front serveru pomocí produktu DCM, jak je uvedeno:
   a) Přistupte k rozhraní DCM, jak je popsáno v tématu “Přístup k DCM” na stránce 268.
   b) V navigačním panelu klepněte na **Výběr úložiště certifikátů**.
      V rámci úlohy se zobrazí stránka Výběr úložiště certifikátů.
   c) Vyberte paměť certifikátů *SYSTEM a klepněte na **Pokračovat**.
   d) V levém panelu rozbalte volbu **Správa aplikací**.
   e) Vyberte definici **Zobrazit aplikaci** a zkontrolujte, zda byl správce front registrován jako aplikace.
      `SSL (WMQ)` je uveden v tabulce.
   f) Vyberte **Aktualizovat přiřazení certifikátu**.
   g) Vyberte **Server** a klepněte na **Pokračovat**.
   h) Vyberte QMGRNAME (WMQ) a klepněte na **Aktualizovat přiřazení certifikátu**.
   i) Vyberte certifikát a klepněte na **Přiřadit nový certifikát**. Otevře se okno se zprávou, že certifikát byl přiřazen k aplikaci.

Obslužný program IBM MQ SSL Client (amqrsslc) pro IBM i

Obslužný program klienta zabezpečení SSL produktu IBM MQ (amqrsslc) pro produkt IBM i je používán produktem IBM MQ MQI client v systémech IBM i k registraci nebo zrušení registrace profilu uživatele klienta nebo k uložení hesla úložiště certifikátů. Obslužný program může být spuštěn pouze uživatelem s profilem se zvláštním oprávněním *ALLOBJ nebo členem QMQMADM, který má volby pro vytvoření nebo odstranění registrace aplikací v DCM (Digital Certificate Manager).

Diagram syntaxe



Registrace profilu uživatele klienta

Pokud IBM MQ MQI client používá paměť certifikátů *SYSTEM, musíte registrovat uživatelský profil klienta (přihlašovací jméno uživatele) pro použití jako aplikace s produktem Digital Certificate Manager (DCM).

Pokud chcete registrovat uživatelský profil klienta, spusťte program **amqrsslc** s volbou `-r` s volbou *UserProfile*. Profil uživatele použitý při volání **amqrsslc** musí mít oprávnění *USE. Zadání *UserProfile* s volbou `-r` registruje *UserProfile* jako serverovou aplikaci s jedinečným popiskem aplikace QIBM_WEBSPHERE_MQ_*UserProfile* a jmenovkou s popisem *UserProfile* (WMQ). Tato serverová aplikace se pak zobrazí v DCM a můžete přiřadit této aplikaci jakýkoli serverový nebo klientský certifikát v systémovém úložišti.

Poznámka: Není-li profil uživatele zadán s volbou `-r` , je zaregistrován uživatelský profil uživatele, který spouští nástroj **amqrsslc** .

Následující kód používá produkt **amqrsslc** k registraci profilu uživatele. V prvním příkladu je registrován uvedený uživatelský profil; ve druhém je 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. Zadání volby *UserProfile* s volbou `-u` zruší registraci *UserProfile* s označením QIBM_WEBSPHERE_MQ_*UserProfile* z DCM.

Poznámka: Není-li profil uživatele zadán s volbou `-u` , odregistruje se uživatel, který spustil nástroj **amqrsslc** .

Následující kód používá produkt **amqrsslc** ke zrušení registrace profilu uživatele. V prvním příkladu je zadaný profil uživatele odregistrován; ve druhém je profil přihlášeného uživatele:

```
CALL PGM(QMQM/AMQRSSLC) PARM('-u' UserProfile)
CALL PGM(QMQM/AMQRSSLC) PARM('-u')
```

Uskladovat heslo k úložišti certifikátů

Pokud IBM MQ MQI client nepoužívá paměť certifikátů *SYSTEM a používá jiné úložiště certifikátů (to znamená, že je hodnota MQSSLKEYR nastavena na jinou hodnotu než *SYSTEM), pak heslo databáze klíčů musí být uloženo. Použijte volbu `-s` pro uložení hesla databáze klíčů na sezavání.

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 vyúží v požadavek na heslo této databáze klíčů. Toto heslo je uloženo v souboru se stejným názvem jako má databáze klíčů s příponou .sth. Tento soubor je uložen na stejné cestě jako databáze klíčů. Příklad kódu generuje soubor stash produktu `/Path/Of/KeyDatabase/MyKey.sth`. QMQM je vlastník uživatele a QMQMADM vlastníka skupiny pro tento soubor. QMQM a QMQMADM mají oprávnění ke čtení, oprávnění k zápisu a jiné profily mají pouze oprávnění ke čtení.

Kdy změny certifikátů nebo paměti certifikátů vstoupí v platnost na IBM i

Změníte-li certifikáty v úložišti certifikátů nebo v umístění úložiště certifikátů, projeví se změny v závislosti na typu kanálu a způsobu, jakým je kanál spuštěn.

Změny certifikátů v úložišti certifikátů a v atributu úložiště klíčů se projeví v následujících situacích:

- Když nový odchozí proces s jedním kanálem poprvé spustí kanál TLS.
- Když nový příchozí proces s jedním kanálem TCP/IP obdrží nejprve požadavek na spuštění kanálu TLS.
- Když je vydán příkaz MQSC REFRESH SECURITY TYPE (SSL) k aktualizaci prostředí IBM MQ TLS.
- V případě klientských aplikací, je-li poslední připojení TLS v procesu zavřeno. Další připojení TLS vyzvedne změny certifikátu.

- V případě kanálů, které jsou spouštěny jako podprocesy procesu fondu procesů (amqrmppa), je-li proces sdružování procesů spuštěn nebo restartován a nejprve spustí kanál TLS. Pokud proces sdružování procesu již má spuštěn kanál TLS a chcete, aby se změna začala okamžitě používat, spusťte příkaz MQSC REFRESH SECURITY TYPE (SSL).
- V případě kanálů, které jsou spuštěny jako podprocesy inicializátoru kanálu, je spuštěn nebo restartován inicializátor kanálu a nejprve se spustí kanál TLS. Pokud proces iniciátoru kanálu již spustil kanál TLS a chcete, aby se změny projevily okamžitě, spusťte příkaz MQSC REFRESH SECURITY TYPE (SSL).
- V případě kanálů, které jsou spuštěny jako podprocesy modulu listener protokolu TCP/IP, je modul listener spuštěn nebo restartován a při prvním přijetí požadavku na spuštění kanálu TLS. Pokud modul listener již spustil kanál TLS a chcete, aby se změny projevily okamžitě, spusťte příkaz MQSC REFRESH SECURITY TYPE (SSL).

Konfigurace kryptografického hardwaru v systému IBM i

Tento postup slouží ke konfiguraci šifrovacího koprocesoru v systému IBM i

Než začnete

Zajistěte, aby váš uživatelský profil měl speciální oprávnění *ALLOBJ a *SECADM, abyste mohli konfigurovat hardware koprocesoru.

Postup

1. Přejděte do adresáře `http://machine.domain:2001` nebo `https://machine.domain:2010`, kde *machine* je název vašeho počítače.

   Zobrazí se dialogové okno s požadavkem na jméno uživatele a heslo.
2. Zadejte platný uživatelský profil a heslo produktu IBM i .
3. Přejděte na volbu Šifrování a postupujte podle příslušných odkazů pro další informace.

Jak pokračovat dále

Další informace o konfiguraci serveru 4767 Cryptographic Coprocessornajdete v tématu 4767 Cryptographic Coprocessor.

ALW Práce s SSL/TLS v AIX, Linux, and Windows

Na systémech AIX, Linux, and Windows je podpora TLS (Transport Layer Security) nainstalována s produktem IBM MQ.

Podrobnější informace o zásadách ověření platnosti certifikátu naleznete v tématu Ověřování platnosti certifikátu a návrh zásad důvěryhodnosti.

ALW *Správa digitálních certifikátů pomocí produktů `runmqckm`, `runmqakma` `strmqikm`*

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

Upozornění: Oba příkazy **`runmqckm`** a **`strmqikm`** se spoléhají na prostředí JRE (Java Runtime Environment) prostředí Java IBM MQ . Pokud v produktu IBM MQ 9.1není prostředí JRE nainstalováno, obdržíte zprávu AMQ9183.

- Linux AIX Pro systémy **AIX and Linux** :
  - Použijte příkaz **`strmqikm`** (iKeyman) ke spuštění grafického uživatelského rozhraní iKeyman .
  - Příkaz **`runmqckm`** se používá k provádění úloh s rozhraním příkazového řádku.
  - K provedení úloh s rozhraním příkazového řádku runmqakm použijte příkaz **`runmqakm`** (GSKCapiCmd). Syntaxe příkazu pro **`runmqakm`** je stejná jako syntaxe pro **`runmqckm`**.

Potřebujete-li spravovat certifikáty TLS způsobem, který vyhovuje standardu FIPS, použijte namísto příkazů **runmqckm** nebo **strmqikm** příkaz **runmqakm** .

Úplný popis rozhraní příkazového řádku pro příkazy **runmqckm** a **runmqakm** najdete v tématu Správa klíčů a certifikátů .

Používáte-li certifikáty nebo klíče uložené na šifrovacím hardwaru PKCS #11 , všimněte si, 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. Pouze 32bitové platformy Windows a Linux x86 jsou jedinými výjimkami, protože programy iKeyman a **runmqckm** jsou na těchto platformách 32bitové.

Další informace viz GSKit: PKCS#11 a IBM MQ režim adresování JRE .

Než spustíte příkaz **strmqikm** ke spuštění grafického uživatelského rozhraní iKeyman , ujistěte se, že pracujete na počítači, který je schopen spustit systém X Window System a že můžete provést následující:

– Nastavte proměnnou prostředí DISPLAY, například:

```
export DISPLAY=mypc:0
```

– Ujistěte se, že proměnná prostředí PATH obsahuje **/usr/bin** a **/bin**. To se také požaduje pro příkazy **runmqckm** a **runmqakm** . Příklad:

```
export PATH=$PATH:/usr/bin:/bin
```

- Windows Pro systémy **Windows** :
  – Ke spuštění grafického uživatelského rozhraní iKeyman použijte příkaz **strmqikm** .
  – Příkaz **runmqckm** se používá k provádění úloh s rozhraním příkazového řádku.

    Potřebujete-li spravovat certifikáty TLS způsobem, který vyhovuje standardu FIPS, použijte namísto příkazů **runmqckm** nebo **strmqikm** příkaz **runmqakm** .
  – Použijte příkaz **runmqakm -keydb** s volbou *stashpw* nebo *stash* .

    Při použití příkazu **runmqakm -keydb** tímto způsobem:

    ```
    runmqakm -keydb -create -db key.kdb -pw secretpwd -stash
    ```

    výsledný soubor `.sth` nemá povolené oprávnění ke čtení pro skupinu `mqm` .

    Tento soubor může číst pouze tvůrce. Po vytvoření souboru pro dočasné ukládání pomocí příkazu **runmqakm** zkontrolujte oprávnění k souboru a udělte oprávnění servisnímu účtu, který spouští správce front, nebo skupině, jako je lokální `mqm`.

ALW Chcete-li požádat o trasování TLS na systémech AIX, Linux, and Windows , prohlédněte si strmqtrc.

Související odkazy

“příkazy runmqckm a runmqakm na systému AIX, Linux, and Windows” na stránce 527
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 produktu **strmqikm** (iKeyman). Grafické rozhraní nebo z příkazového řádku pomocí příkazů **runmqckm** (iKeycmd) nebo **runmqakm** (GSKCapiCmd).

Informace o této úloze

Připojení TLS vyžaduje *úložiště klíčů* na každém konci připojení. Každý správce front produktu IBM MQ a produkt IBM MQ MQI client musí mít přístup k úložišti klíčů. Další informace viz "Úložiště klíčů SSL/TLS" na stránce 23.

V systému 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 štítky. Specifický popisek asociuje osobní certifikát se správcem front nebo IBM MQ MQI client. TLS používá tento certifikát pro účely autentizace. Na systémech AIX, Linux, and Windows používá produkt IBM MQ hodnotu atributu **CERTLABL** (pokud je nastavena) nebo standardní `ibmwebspheremq` s připojeným jménem správce front nebo přihlašovacího ID uživatele IBM MQ MQI client , vše malými písmeny. Podrobnosti najdete v tématu Digitální certifikáty certifikátu .

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`.

  V 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`.

  Výchozí název kmene je `key`. Volitelně si můžete vybrat vlastní cestu a název kmene, ale rozšíření musí být `.kdb`.

  Pokud vyberete svou vlastní cestu nebo název souboru, nastavte oprávnění k souboru tak, aby k němu měl přístup těsně pod kontrolou.
- Pro klienta IBM MQ neexistuje žádná výchozí cesta nebo název kmene. Ulehčeně řídit přístup k tomuto souboru. Rozšíření musí být `.kdb`.

Nevytvářejte klíčová úložiště na systému souborů, který nepodporuje zámky na úrovni souboru, například NFS verze 2 na systémech Linux .

Informace o kontrole a určení názvu souboru databáze klíčů viz "Změna umístění úložiště klíčů pro správce front v systému AIX, Linux, and Windows" na stránce 285 . Název souboru databáze klíčů můžete zadat buď před vytvořením databázového souboru klíčů, nebo po něm.

ID uživatele, ze kterého spouštíte příkazy **strmqikm** nebo **runmqckm** , musí mít oprávnění k zápisu do adresáře, ve kterém je soubor databáze klíčů vytvořen nebo aktualizován. Pro správce front, který používá výchozí adresář `ssl` , musí být ID uživatele, ze kterého spouštíte produkt **strmqikm** nebo **runmqckm** , členem skupiny mqm. Pokud u produktu IBM MQ MQI clientspustíte příkaz **strmqikm** nebo **runmqckm** z jiného ID uživatele, než je ID uživatele, pod nímž je klient spuštěn, musíte změnit oprávnění k souboru, aby mohl produkt IBM MQ MQI client přistupovat k souboru databáze klíčů za běhu programu. Další informace viz "Přístup k databázovým souborům a jejich zabezpečení v systému Windows" na stránce 283 nebo "Přístup k databázovým souborům a jejich zabezpečení v systémech AIX and Linux" na stránce 283.

V produktu **strmqikm** nebo **runmqckm** for GSKit 7.0jsou nové databáze klíčů automaticky naplněny sadou předem definovaných certifikátů certifikačních autorit (CA). Databáze klíčů v produktu **strmqikm** nebo **runmqckm** for GSKit 8.0nejsou automaticky naplněny daty, takže počáteční nastavení je bezpečnější, protože do souboru databáze klíčů zahrnete pouze ty certifikáty CA, které chcete.

Poznámka: Vzhledem k tomu, že tato změna v chování pro GSKit 8.0 vede k automatickému přidání certifikátů CA do úložiště, musíte ručně přidat upřednostňované certifikáty CA. Tato změna chování vám poskytuje přesnější a detailnější kontrolu nad použitními certifikáty CA. Viz téma "Přidání výchozích certifikátů CA do prázdného úložiště klíčů v systému AIX, Linux, and Windows s produktem GSKit 8.0" na stránce 284.

Databázi klíčů vytvoříte buď pomocí příkazového řádku, nebo pomocí uživatelského rozhraní produktu **strmqikm** (iKeyman).

Poznámka: Musíte-li spravovat certifikáty TLS způsobem, který je kompatibilní se standardem FIPS-, použijte příkaz **runmqakm** . Uživatelské rozhraní produktu **strmqikm** neposkytuje volbu vyhovující FIPS.

Postup

Vytvořte databázi klíčů pomocí příkazového řádku.

1. Spusťte některý z následujících příkazů:

   - Použití **runmqckm**:

     ```
     runmqckm -keydb -create -db filename -pw password -type cms -stash
     ```

   - Použití **runmqakm**:

     ```
     runmqakm -keydb -create -db filename -pw password -type cms
     -stash -fips -strong
     ```

   kde:

   -db *název_souboru*
   Uvádí plně kvalifikovaný název souboru databáze klíčů CMS a musí mít příponu souboru .kdb.

   -pw *heslo*
   Určuje heslo pro databázi klíčů CMS.

   -type *cms*
   Uvádí typ databáze. (Pro IBM MQmusí být cms.)

   -stash
   Uloží heslo databáze klíčů do souboru.

   -fips
   určuje, že příkaz má být spuštěn v režimu FIPS. Při použití režimu FIPS komponenta ICC používá algoritmy, které jsou validovány FIPS 140-2. Pokud se komponenta ICC neinicializuje v režimu FIPS, příkaz **runmqakm** se nezdaří.

   -silné
   Kontroluje, zda zadané heslo splňuje minimální požadavky na odolnost hesla. Minimální požadavky na heslo jsou tyto:

   - Heslo musí mít minimální délku 14 znaků.
   - Heslo musí obsahovat minimálně jedno malé písmeno, jedno velké písmeno a jednu číslici nebo speciální znak. Mezi speciální znaky patří hvězdička (*), znak dolaru ($), symbol čísla (#) a znak procenta (%). Prostor je klasifikován jako speciální znak.
   - Každý znak může v hesle nastat maximálně třikrát.
   - Maximální počet dvou po sobě jdoucích znaků v hesle může být stejný.
   - Všechny znaky jsou ve standardním tisknutelném znakové sadě ASCII, v rozsahu 0x20 - 0x7E.

Volitelně můžete vytvořit databázi klíčů pomocí uživatelského rozhraní produktu **strmqikm** (iKeyman).

2. V systémech AIX and Linux se přihlaste jako uživatel root. V systému 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 nové okno.
5. Klepněte na volbu **Typ databáze klíčů** a vyberte položku **CMS** (Certificate Management System).
6. Do pole **Název souboru** zadejte název souboru.

   Toto pole již obsahuje text key.kdb. Pokud je váš název kmene key, ponechte toto pole nezměněné. Pokud jste uvedli jiný název souboru, nahraďte key svým kmenovým jménem. Rozšíření .kdb však nesmíte změnit.
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 se musí shodovat s hodnotou atributu **SSLKeyRepository** správce front.
- Pro klienta IBM MQ : `/var/mqm/ssl` (v systémech AIX and Linux) nebo `C:\mqm\ssl` (v systémech Windows).

8. Klepněte na tlačítko **OK**.

   Otevře se okno Výzva k zadání hesla.
9. Do pole **Heslo** zadejte heslo a zadejte je znovu do pole **Potvrdit heslo** .
10. Vyberte zaškrtávací políčko **Stash heslo do souboru** .

    Poznámka: Pokud heslo neschováte, pokusy o spuštění kanálů TLS selžou, protože nemohou získat heslo potřebné pro přístup k souboru databáze klíčů.
11. Klepněte na tlačítko **OK**.

    Otevře se okno Osobní certifikáty.
12. Nastavte přístupová oprávnění podle popisu v části "Přístup k databázovým souborům a jejich zabezpečení v systému Windows" na stránce 283 nebo "Přístup k databázovým souborům a jejich zabezpečení v systémech AIX and Linux" na stránce 283.

Windows *Přístup k databázovým souborům a jejich zabezpečení v systému Windows*

Soubory databáze klíčů nemusí mít příslušná přístupová oprávnění. Musíte nastavit odpovídající přístup k těmto souborům.

Nastavte řízení přístupu na soubory *key*.kdb, *key*.sth, *key*.crla *key*.rdb, kde *klíč* je název kmene vaší databáze klíčů, čímž udělíte oprávnění k omezené sadě uživatelů.

Zvažte udělení přístupu následujícím způsobem:

úplné oprávnění
BUILTIN\Administrators, NT AUTHORITY\SYSTEM a uživatel, který vytvořil databázové soubory.

oprávnění ke čtení
Pouze pro správce front, pouze lokální skupinu mqm. Předpokládá se, že agent MCA je spuštěn pod ID uživatele ve skupině mqm.

Pro klienta se jedná o ID uživatele, pod kterým je spuštěn proces klienta.

Linux AIX *Přístup k databázovým souborům a jejich zabezpečení v systémech AIX and Linux*

Soubory databáze klíčů nemusí mít příslušná přístupová oprávnění. Musíte nastavit odpovídající přístup k těmto souborům.

Pro správce front nastavte oprávnění k souborům databáze klíčů tak, aby je správce front a procesy kanálů mohly v případě potřeby číst, ale ostatní uživatelé je nemohou číst nebo upravovat. Za normálních okolností potřebuje uživatel mqm oprávnění ke čtení. Pokud jste vytvořili soubor databáze klíčů tak, že se přihlásíte jako uživatel mqm, budou pravděpodobně dostatečná oprávnění; pokud jste nebyli uživatelem mqm, ale jiným uživatelem ve skupině mqm, pravděpodobně budete muset udělit oprávnění ke čtení jiným uživatelům ve skupině mqm.

Podobně jako u klienta nastavte oprávnění k souborům databáze klíčů tak, aby je v případě potřeby mohly procesy klientské aplikace číst, ale ostatní uživatelé je nemohou číst nebo upravovat. Za normálních okolností je uživatel, pod kterým proces klienta spouští, nutná oprávnění ke čtení. Pokud jste vytvořili soubor databáze klíčů tak, že se přihlásíte jako tento uživatel, pak jsou oprávnění pravděpodobně dostatečná; pokud jste nebyli uživatelé klienta procesu, ale jiný uživatel v této skupině, pravděpodobně budete muset udělit oprávnění ke čtení ostatním uživatelům ve skupině.

Nastavte oprávnění u souborů *key*.kdb, *key*.sth, *key*.crla *key*.rdb, kde *klíč* je název kmene vaší databáze klíčů, pro čtení a zápis pro vlastníka souboru a pro čtení pro skupinu mqm nebo skupinu uživatelů klienta (-rw-r -----).

ALW *Přidání výchozích certifikátů CA do prázdného úložiště klíčů v systému AIX, Linux, and Windows s produktem GSKit 8.0*

Chcete-li přidat jeden nebo více výchozích certifikátů CA do prázdného úložiště klíčů s produktem GSKit 8.0, postupujte podle této procedury.

V produktu GSKit 7.0bylo chování při vytváření nového úložiště klíčů automaticky přidáno v sadě výchozích certifikátů CA pro běžně používaná certifikační autority. U produktu GSKit 8.0se toto chování změnilo, takže certifikáty certifikační autority již nebudou automaticky přidány 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** (v 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, 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 **Naplnit**. Otevře se okno Přidání certifikátu CA.
10. Certifikáty CA, které jsou k dispozici pro přidání do úložiště, jsou zobrazeny v hierarchické stromové struktuře. Vyberte položku nejvyšší úrovně pro organizaci, jejíž certifikáty CA chcete důvěřovat, abyste zobrazili úplný seznam platných certifikátů CA.
11. Vyberte certifikáty CA, kterým chcete důvěřovat ze seznamu, a klepněte na **OK**. Certifikáty se přidají do úložiště klíčů.

z příkazového řádku,

Pomocí následujících příkazů zobrazte seznam a poté přidejte certifikáty CA pomocí produktu **runmqckm**:

- Vydejte následující příkaz, který vypíše výchozí certifikáty CA spolu s organizacemi, které je vydávají:

```
runmqckm -cert -listsigners
```

- Chcete-li přidat všechny certifikáty CA pro organizaci uvedenou v poli *label* , zadejte následující příkaz:

```
runmqckm -cert -populate -db filename -pw password -label label
```

kde:

`-db` *filename*	je úplná cesta k databázi 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 daným certifikátem CA. Pečlivě zvažte, které certifikační autority chcete důvěřovat, a přidejte pouze sadu certifikátů CA potřebných k ověření klientů a správců. Nedoporučuje se přidávat plnou sadu výchozích certifikátů CA, pokud to není definitivní požadavek pro vaši strategii zabezpečení.

ALW *Vyhledání úložiště klíčů pro správce front v systému AIX, Linux, and Windows*

Tento postup slouží k získání umístění souboru databáze klíčů správce front.

Postup

1. Zobrazte atributy správce front pomocí jednoho z následujících příkazů MQSC:

```
DISPLAY QMGR ALL
DISPLAY QMGR SSLKEYR
```

   Atributy správce front můžete také zobrazit pomocí příkazů IBM MQ Explorer nebo PCF.
2. Prověřte výstup příkazu pro cestu a název stem databázového souboru 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 .

ALW *Změna umístění úložiště klíčů pro správce front v systému AIX, Linux, and Windows*

Umístění souboru databáze klíčů správce front lze změnit pomocí různých způsobů, včetně příkazu MQSC ALTER QMGR.

Umístění souboru databáze klíčů správce front lze změnit pomocí příkazu MQSC příkazu ALTER QMGR a nastavit atribut úložiště klíčů správce front. Například v systému AIX and Linux:

```
ALTER QMGR SSLKEYR('/var/mqm/qmgrs/QM1/ssl/MyKey')
```

Soubor databáze klíčů má úplný název souboru: `/var/mqm/qmgrs/QM1/ssl/MyKey.kdb`

V systému Windows:

```
ALTER QMGR SSLKEYR('C:\Program Files\IBM\MQ\Qmgrs\QM1\ssl\Mykey')
```

Soubor databáze klíčů má úplný název souboru: `C:\Program Files\IBM\MQ\Qmgrs\QM1\ssl\Mykey.kdb`

Upozornění: Ujistěte se, že jste nezahrnuli příponu `.kdb` do názvu souboru v klíčovém slově SSLKEYR, protože správce front toto rozšíření připojí automaticky.

Atributy správce front můžete také změnit pomocí příkazů programu Průzkumník IBM MQ nebo PCF.

Změníte-li umístění souboru databáze klíčů správce front, nebudou certifikáty přeneseny ze starého umístění. Je-li klíčovým databázovým souborem, k němuž nyní přistupujete, nový soubor databáze klíčů, musíte jej naplnit daty CA a osobními certifikáty, které potřebujete, jak je popsáno v tématu “Import osobního certifikátu do úložiště klíčů v systému AIX, Linux, and Windows” na stránce 300.

ALW *Nalezení klíčového úložiště pro IBM MQ MQI client v systému AIX, Linux, and Windows*

Umístění úložiště klíčů je dáno proměnnou MQSSLKEYR nebo zadanou v rámci volání MQCONNX.

Prověřte proměnnou prostředí MQSSLKEYR a vyhledejte umístění souboru databáze klíčů pro produkt IBM MQ MQI client. Příklad:

```
echo $MQSSLKEYR
```

Zkontrolujte také svou aplikaci, protože název souboru databáze klíčů lze také nastavit v rámci volání MQCONNX, jak je popsáno v tématu"Určení umístění úložiště klíčů pro IBM MQ MQI client v systému AIX, Linux, and Windows" na stránce 286. Hodnota nastavená ve volání MQCONNX přepíše hodnotu proměnné MQSSLKEYR.

ALW *Určení umístění úložiště klíčů pro IBM MQ MQI client v systému AIX, Linux, and Windows*

Pro IBM MQ MQI clientneexistuje žádné výchozí úložiště klíčů. Jeho umístění můžete zadat jedním ze dvou způsobů. Ujistěte se, že k souboru databáze klíčů lze přistupovat pouze určeným uživatelům nebo administrátorům, aby se zabránilo neoprávněnému kopírování do jiných systémů.

Umístění souboru databáze klíčů pro produkt IBM MQ MQI client můžete určit dvěma způsoby:

- Nastavení proměnné prostředí MQSSLKEYR. Například v systému AIX and Linux:

  ```
  export MQSSLKEYR=/var/mqm/ssl/key
  ```

  Soubor databáze klíčů má plně kvalifikovaný název souboru:

  ```
  /var/mqm/ssl/key.kdb
  ```

  V systému Windows:

  ```
  set MQSSLKEYR=C:\Program Files\IBM\MQ\ssl\key
  ```

  Soubor databáze klíčů má plně kvalifikovaný název souboru:

  ```
  C:\Program Files\IBM\MQ\ssl\key.kdb
  ```

  Poznámka: Přípona .kdb je povinná část názvu souboru, ale není zahrnuta jako část hodnoty proměnné prostředí.

- Zadání cesty a názvu souboru databáze klíčů v poli *KeyRepository* struktury MQSCO při volání MQCONNX při volání aplikace MQCONNX. Další informace o použití struktury MQSCO v MQCONNX najdete v tématu Přehled pro MQSCO.

ALW *Kdy změny certifikátů nebo paměti certifikátů vstoupí v platnost na AIX, Linux, and Windows*

Změníte-li certifikáty v úložišti certifikátů nebo v umístění úložiště certifikátů, projeví se změny v závislosti na typu kanálu a způsobu, jakým je kanál spuštěn.

Změny v certifikátech v souboru databáze klíčů a v atributu úložiště klíčů se stanou platnými v následujících situacích:

- Když nový odchozí proces s jedním kanálem poprvé spustí kanál TLS.
- Když nový příchozí proces s jedním kanálem TCP/IP obdrží nejprve požadavek na spuštění kanálu TLS.
- Když je vydán příkaz MQSC REFRESH SECURITY TYPE (SSL), aby se aktualizování prostředí TLS aktualizování.
- V případě klientských aplikací, je-li poslední připojení TLS v procesu zavřeno. Další připojení TLS vyzvedne změny certifikátu.

- V případě kanálů, které jsou spouštěny jako podprocesy procesu fondu procesů (amqrmppa), je-li proces sdružování procesů spuštěn nebo restartován a nejprve spustí kanál TLS. Pokud proces sdružování procesu již má spuštěn kanál TLS a chcete, aby se změna začala okamžitě používat, spusťte příkaz MQSC REFRESH SECURITY TYPE (SSL).
- V případě kanálů, které jsou spuštěny jako podprocesy inicializátoru kanálu, je spuštěn nebo restartován inicializátor kanálu a nejprve se spustí kanál TLS. Pokud proces iniciátoru kanálu již spustil kanál TLS a chcete, aby se změny projevily okamžitě, spusťte příkaz MQSC REFRESH SECURITY TYPE (SSL).
- V případě kanálů, které jsou spuštěny jako podprocesy modulu listener protokolu TCP/IP, je modul listener spuštěn nebo restartován a při prvním přijetí požadavku na spuštění kanálu TLS. Pokud modul listener již spustil kanál TLS a chcete, aby se změny projevily okamžitě, spusťte příkaz MQSC REFRESH SECURITY TYPE (SSL).

Prostředí produktu IBM MQ TLS můžete aktualizovat také pomocí příkazů programu Průzkumník IBM MQ nebo PCF.

ALW *Vytvoření osobního certifikátu podepsaného sebou samým na serveru AIX, Linux, and Windows*

Certifikát s automatickým podpisem můžete vytvořit pomocí **strmqikm** (iKeyman) GUI, 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 .

Názvy algoritmů digitálního podpisu SHA3WithRSA a SHA5WithRSA jsou zamítnuty, protože se jedná o zkrácený tvar SHA384WithRSA a SHA512WithRSA .

Další informace o důvodech použití certifikátů s vlastním podpisem naleznete v tématu Použití certifikátů podepsaných držitelem pro vzájemné ověření 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. Podrobné informace naleznete v tématu “Interoperabilita specifikací Elliptic Curve a RSA CipherSpecs” na stránce 44 v tématu “Digitální certifikáty a kompatibilita CipherSpec v produktu IBM MQ” na stránce 43 .

Chcete-li použít typ 1 CipherSpecs (jména s názvy začínajícími ECDHE_ECDSA_), musíte použít příkaz **runmqakm** k vytvoření certifikátu a musíte zadat parametr podpisového algoritmu ECDSA Elliptic Curve; například **-sig_alg** EC_ecdsa_with_SHA384.

Seznam voleb, které jsou k dispozici s algoritmem hašování **-sig_alg** , naleznete v části “Volby runmqckm a runmqakm na systému AIX, Linux, and Windows” na stránce 541 .

Pokud používáte:

- Grafické rozhraní, viz “Použití uživatelského rozhraní produktu strmqikm” na stránce 287
- Příkazový řádek, viz “z příkazového řádku,” na stránce 288

ALW *Použití uživatelského rozhraní produktu **strmqikm***

Osobní certifikát můžete vytvořit pomocí produktu **strmqikm** (iKeyman). -GII.

Informace o této úloze

strmqikm neposkytuje volbu vyhovující FIPS. Potřebujete-li spravovat certifikáty TLS způsobem, který je kompatibilní se standardem FIPS-, použijte příkaz **runmqakm** .

Postup

Chcete-li vytvořit osobní certifikát pro správce front nebo produkt IBM MQ MQI client pomocí grafického uživatelského rozhraní, proveďte následující kroky:

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 generovat 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 databázového souboru databáze se zobrazí v poli **Název souboru** .
8. V nabídce **Vytvořit** klepněte na **Nový certifikát podepsaný svým držitelem**. Zobrazí se okno Vytvoření nového certifikátu podepsaného sám sebou.
9. Do pole **Jmenovka klíče** zadejte jmenovku certifikátu.
   Jmenovka je buď hodnota atributu **CERTLABL** , je-li nastavena, nebo standardní `ibmwebspheremq` s připojeným jménem správce front nebo IBM MQ MQI client ID uživatele pro přihlášení, vše malými písmeny. Podrobnosti najdete v tématu Digitální certifikáty certifikátu .
10. Zadejte nebo vyberte hodnotu pro libovolné pole v poli **Rozlišovací jméno** nebo kterékoliv z polí **Alternativní jméno subjektu** .
11. U zbývajících polí buď přijměte výchozí hodnoty, nebo zadejte nové hodnoty nebo vyberte nové hodnoty.
    Další informace o rozlišujících názvech naleznete v tématu “Rozlišující názvy” na stránce 11.
12. Klepněte na tlačítko **OK**.
    Seznam **Osobní certifikáty** zobrazuje štítek osobního certifikátu podepsaného sebou samým, který jste vytvořili sami.

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 je kompatibilní se standardem FIPS-, použijte příkaz **runmqakm** .

Postup

Vytvořte osobní certifikát podepsaný držitelem pomocí příkazuGSKCapiCmd(**runmqckm** nebo **runmqakm**).

- 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***
Uvádí plně kvalifikovaný název souboru databáze klíčů CMS.

-pw ***heslo***
Určuje heslo pro databázi klíčů CMS.

-label ***popisek***
Určuje jmenovku klíče připojenou k certifikátu. Návěští je buď hodnota atributu **CERTLABL** , pokud je nastavena, nebo standardní `ibmwebspheremq` s názvem správce front nebo přihlašovacím jménem uživatele IBM MQ MQI client , které jsou připojeny, vše malými písmeny. Podrobnosti viz “Digitální certifikáty certifikátu, základní informace o požadavcích” na stránce 24.

-dn ***rozlišující_název***
Určuje rozlišující název X.500 uzavřený ve dvojitých uvozovkách. Je povinný alespoň jeden atribut. Můžete zadat více atributů OU a DC.

Poznámka: Nástroje **runmqckm** a **runmqakm** odkazují na atribut PSČ jako `POSTALCODE`, nikoli na PC. Vždy zadejte `POSTALCODE` do parametru **-dn** , když použijete tyto příkazy správy certifikátů k vyžádání certifikátů s poštovním směrovači.

-size ***velikost_klíče***
Určuje velikost klíče. Pokud používáte produkt **runmqckm**, hodnota může být 512 nebo 1024. Pokud používáte produkt **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***
Doba vypršení platnosti ve dnech certifikátu. Předvolba je 365 dní pro certifikát.

-fips
určuje, že příkaz má být spuštěn v režimu FIPS. Je použita pouze komponenta FIPS ICC a tato komponenta musí být úspěšně inicializována v režimu FIPS. V režimu FIPS komponenta ICC používá algoritmy ověřené dle standardu FIPS 140-2. Pokud se komponenta ICC neinicializuje v režimu FIPS, příkaz **runmqakm** se nezdaří.

-sig_alg
Pro **runmqckm**uvádí asymetrický podpisový algoritmus použitý pro vytvoření dvojice klíčů položky. The value can be, `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 produkt **runmqakm**určuje algoritmus hašování použitý při vytváření žádosti o certifikát. Tento algoritmus hašování se používá k vytvoření podpisu přidruženého k nově vytvořené žádosti o certifikát. The value can be `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_SHA384`, or `EC_ecdsa_with_SHA512`. Výchozí hodnota je `SHA1WithRSA`.

-san_dnsname ***DNS_názvy***
Určuje seznam názvů DNS oddělených čárkami pro vytvářená položka, které jsou odděleny čárkami nebo mezerami jako oddělovači.

-san_emailaddr ***e-mailové_adresy***
Určuje seznam e-mailových adres oddělených čárkami pro vytvářený záznam, oddělený čárkami nebo mezerami jako oddělovači.

-san_ipaddr ***adresa_IP***
Určuje seznam adres IP oddělených čárkami pro vytvářený záznam, oddělený čárkami nebo mezerami jako oddělovači.

ALW *Požádání o osobní certifikát v systému AIX, Linux, and Windows*

Osobní certifikát můžete požádat pomocí produktu **strmqikm** (iKeyman) Grafické rozhraní nebo z příkazového řádku pomocí příkazů **runmqckm** (iKeycmd) nebo **runmqakm** (GSKCapiCmd). Potřebujete-li spravovat certifikáty SSL nebo TLS způsobem, který je kompatibilní se standardem FIPS-, použijte příkaz **runmqakm** .

Informace o této úloze

Osobní certifikát můžete požádat buď pomocí grafického uživatelského rozhraní produktu **strmqikm** , nebo z příkazového řádku, a to s následujícími úvahami:

- 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 .
- Názvy algoritmů digitálního podpisu SHA3WithRSA a SHA5WithRSA jsou zamítnuty, protože se jedná o zkrácený tvar SHA384WithRSA a SHA512WithRSA .
- Ne všechny digitální certifikáty lze použít se všemi CipherSpecs. Ujistěte se, že požadujete certifikát kompatibilní se specifikacemi CipherSpecs , které potřebujete použít. Produkt IBM MQ podporuje tři různé typy CipherSpec. Podrobné informace naleznete v tématu “Interoperabilita specifikací Elliptic Curve a RSA CipherSpecs” na stránce 44 v tématu “Digitální certifikáty a kompatibilita CipherSpec v produktu IBM MQ” na stránce 43 .
- Chcete-li použít typ 1 CipherSpecs (s názvy začínajícími ECDHE_ECDSA_), musíte použít příkaz **runmqakm** k vyžádání certifikátu a musíte zadat parametr podpisového algoritmu ECDSA Elliptic Curve; například **-sig_alg** EC_ecdsa_with_SHA384.

  Seznam voleb, které jsou k dispozici s algoritmem hašování **-sig_alg** , naleznete v části “Volby runmqckm a runmqakm na systému AIX, Linux, and Windows” na stránce 541 .
- Pouze příkaz **runmqakm** poskytuje volbu vyhovující FIPS.
- Používáte-li kryptografický hardware, přečtěte si téma “Požádání o osobní certifikát pro hardware PKCS #11” na stránce 308.

Pokud používáte:

- Grafické rozhraní, viz “Použití uživatelského rozhraní produktu strmqikm” na stránce 290
- Příkazový řádek, viz “z příkazového řádku,” na stránce 291

ALW *Použití uživatelského rozhraní produktu **strmqikm***

Osobní certifikát můžete požádat pomocí produktu **strmqikm** (iKeyman) -GII. Potřebujete-li spravovat certifikáty SSL nebo TLS způsobem, který je kompatibilní se standardem FIPS-, použijte příkaz **runmqakm** .

Informace o této úloze

strmqikm neposkytuje volbu vyhovující FIPS. Potřebujete-li spravovat certifikáty TLS způsobem, který je kompatibilní se standardem FIPS-, použijte příkaz **runmqakm** .

Postup

Chcete-li požádat o osobní certifikát pomocí uživatelského rozhraní iKeyman , proveďte následující kroky:

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 generovat 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 databázového souboru databáze se zobrazí v poli **Název souboru** .
8. V nabídce **Vytvořit** klepněte na **Nový požadavek na certifikát**. Otevře se okno **Vytvořit nový klíč a žádost o certifikát** .
9. Do pole **Jmenovka klíče** zadejte jmenovku certifikátu.

   Jmenovka je buď hodnota atributu **CERTLABL** , je-li nastavena, nebo standardní `ibmwebspheremq` s připojeným jménem správce front nebo IBM MQ MQI client ID uživatele pro přihlášení, vše malými písmeny. Podrobnosti najdete v tématu Digitální certifikáty certifikátu .
10. Zadejte nebo vyberte hodnotu pro libovolné pole v poli **Rozlišovací jméno** nebo kterékoliv z polí **Alternativní jméno subjektu** . U zbývajících polí buď přijměte výchozí hodnoty, nebo zadejte nové hodnoty nebo vyberte nové hodnoty.

    Další informace o rozlišujících názvech naleznete v tématu “Rozlišující názvy” na stránce 11.
11. Do pole **Zadejte název souboru, do kterého chcete uložit žádost o certifikát** , buď přijměte výchozí `certreq.arm`, nebo zadejte novou hodnotu s úplnou cestou.
12. Klepněte na tlačítko **OK**.

    Zobrazí se potvrzovací okno.
13. Klepněte na tlačítko **OK**.

    V seznamu **Požadavky na osobní certifikáty** je zobrazen popisek nové žádosti o osobní certifikát, kterou jste vytvořili. Požadavek na certifikát je uložen v souboru, který jste zvolili v kroku “11” na stránce 291.
14. Vyžádejte si nový osobní certifikát odesláním souboru certifikační autoritě (CA) nebo zkopírováním souboru do formuláře požadavku na webovém serveru pro CA.

ALW *z příkazového řádku,*

Můžete požádat o osobní certifikát z příkazového řádku pomocí příkazů **runmqckm** (iKeycmd) nebo **runmqakm** (GSKCapiCmd). Potřebujete-li spravovat certifikáty SSL nebo TLS způsobem, který je kompatibilní se standardem FIPS-, použijte příkaz **runmqakm** .

Postup

Požádejte o 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***
: Uvádí plně kvalifikovaný název souboru databáze klíčů CMS.

-pw ***heslo***
: Určuje heslo pro databázi klíčů CMS.

-label *popisek*
Určuje jmenovku klíče připojenou k certifikátu. Návěští je buď hodnota atributu **CERTLABL** , pokud je nastavena, nebo standardní `ibmwebspheremq` s názvem správce front nebo přihlašovacím jménem uživatele IBM MQ MQI client , které jsou připojeny, vše malými písmeny. Podrobnosti viz “Digitální certifikáty certifikátu, základní informace o požadavcích” na stránce 24.

-dn *rozlišující_název*
Určuje rozlišující název X.500 uzavřený ve dvojitých uvozovkách. Je povinný alespoň jeden atribut. Můžete zadat více atributů OU a DC.

Poznámka: Nástroje **runmqckm** a **runmqakm** odkazují na atribut PSČ jako POSTALCODE, nikoli na PC. Vždy zadejte POSTALCODE do parametru **-dn** , když použijete tyto příkazy správy certifikátů k vyžádání certifikátů s poštovním směrovači.

-size *velikost_klíče*
Určuje velikost klíče. Pokud používáte produkt **runmqckm**, hodnota může být 512 nebo 1024. Pokud používáte produkt **runmqakm**, hodnota může být 512, 1024nebo 2048.

-file *název_souboru*
Určuje název souboru pro žádost o certifikát.

-fips
určuje, že příkaz má být spuštěn v režimu FIPS. Při použití režimu FIPS komponenta ICC používá algoritmy, které jsou validovány FIPS 140-2. Pokud se komponenta ICC neinicializuje v režimu FIPS, příkaz **runmqakm** se nezdaří.

-sig_alg
Pro **runmqckm**uvádí asymetrický podpisový algoritmus použitý pro vytvoření dvojice klíčů položky. The value can be, `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 produkt **runmqakm**určuje algoritmus hašování použitý při vytváření žádosti o certifikát. Tento algoritmus hašování se používá k vytvoření podpisu přidruženého k nově vytvořené žádosti o certifikát. The value can be `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_SHA384`, or `EC_ecdsa_with_SHA512`. Výchozí hodnota je `SHA1WithRSA`.

-san_dnsname *DNS_názvy*
Určuje seznam názvů DNS oddělených čárkami pro vytvářená položka, které jsou odděleny čárkami nebo mezerami jako oddělovači.

-san_emailaddr *e-mailové_adresy*
Určuje seznam e-mailových adres oddělených čárkami pro vytvářený záznam, oddělený čárkami nebo mezerami jako oddělovači.

-san_ipaddr *adresa_IP*
Určuje seznam adres IP oddělených čárkami pro vytvářený záznam, oddělený čárkami nebo mezerami jako oddělovači.

Jak pokračovat dále

Odešlete žádost o certifikát certifikační autoritě. Další informace viz “Přijímání osobních certifikátů do úložiště klíčů v systému AIX, Linux, and Windows” na stránce 294.

ALW *Obnova existujícího osobního certifikátu v systému AIX, Linux, and Windows*

Osobní certifikát můžete obnovit pomocí produktu **strmqikm** (iKeyman). Grafické rozhraní nebo z příkazového řádku pomocí příkazů **runmqckm** (iKeycmd) nebo **runmqakm** (GSKCapiCmd).

Informace o této úloze

Máte-li požadavek používat větší velikosti klíčů pro vaše osobní certifikáty, nemůžete obnovit existující certifikát. You must replace your existing key by following the steps described in "Požádání o osobní certifikát v systému AIX, Linux, and Windows" na stránce 290 to create a new certificate request that uses the key sizes you require.

Osobní certifikát má datum vypršení platnosti, po jehož uplynutí již nebude možné certifikát používat. Tato úloha vysvětluje, jak obnovit existující osobní certifikát dříve, než vyprší.

*Použití uživatelského rozhraní produktu **strmqikm***

Informace o této úloze

strmqikm neposkytuje volbu vyhovující FIPS. Potřebujete-li spravovat certifikáty TLS způsobem, který je kompatibilní se standardem FIPS-, použijte příkaz **runmqakm** .

Postup

Chcete-li požádat o osobní certifikát pomocí uživatelského rozhraní produktu **strmqikm** , proveďte následující kroky:

1. Spusťte uživatelské rozhraní pomocí příkazu **strmqikm** v 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 generovat 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 databázového souboru databáze se zobrazí v poli **Název souboru** .
8. Vyberte položku **Osobní certifikáty** z rozevírací nabídky pro výběr a vyberte certifikát ze seznamu, který chcete obnovit.
9. Klepněte na volbu **Znovu vytvořit požadavek ...** tlačítko.
   Otevře se okno, kde můžete zadat informace o názvu souboru a umístění souboru.
10. V poli **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 se uloží do souboru, který jste vybrali v kroku "9" na stránce 293.
12. Vyžádejte si nový osobní certifikát odesláním souboru certifikační autoritě (CA) nebo zkopírováním souboru do formuláře požadavku na webovém serveru pro CA.

z příkazového řádku,

Postup

Chcete-li požádat o osobní certifikát pomocí příkazu **runmqckm** nebo **runmqakm** , použijte následující příkazy:

- Použití **runmqckm**:

```
runmqckm -certreq -recreate -db filename -pw
password -label label
-target filename
```

- Použití runmqakm:

```
runmqakm -certreq -recreate -db filename -pw
password -label label
-target filename
```

kde:

-db ***název_souboru***
Uvádí plně kvalifikovaný název souboru databáze klíčů CMS.

-pw ***heslo***
Určuje heslo pro databázi klíčů CMS.

-target ***název_souboru***
Určuje název souboru pro žádost o certifikát.

Jak pokračovat dále

Jakmile obdržíte podepsaný osobní certifikát od certifikační autority, můžete jej přidat do své databáze klíčů pomocí postupu popsaného v tématu “Přijímání osobních certifikátů do úložiště klíčů v systému AIX, Linux, and Windows” na stránce 294.

ALW *Přijímání osobních certifikátů do úložiště klíčů v systému AIX, Linux, and Windows*

Tento postup použijte k přijetí osobního certifikátu do souboru databáze klíčů. Úložiště klíčů musí být stejné jako úložiště, ve kterém jste vytvořili žádost o certifikát.

Poté, co vám CA pošle nový osobní certifikát, přidáte jej do souboru databáze klíčů, ze kterého jste generovali novou žádost o certifikát. Pokud CA odešle certifikát jako část e-mailové zprávy, zkopírujte tento certifikát do samostatného souboru.

Použití produktu **strmqikm**

Potřebujete-li spravovat certifikáty TLS způsobem, který vyhovuje standardu FIPS, použijte příkaz **runmqakm** . **strmqikm** neposkytuje volbu vyhovující FIPS.

Ujistěte se, že soubor certifikátů, který má být importován, má oprávnění k zápisu pro aktuálního uživatele, a pak použijte následující proceduru buď pro správce front, nebo pro IBM MQ MQI client , aby přijal osobní certifikát 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 tlačítko **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 zobrazení **Osobní certifikáty** .
8. Klepněte na tlačítko **Přijmout**. Otevře se okno Přijmout certifikát ze souboru.
9. Zadejte název souboru certifikátu a umístění pro nový osobní certifikát, nebo klepněte na tlačítko **Procházet** a vyberte název a umístění.

10. Klepněte na tlačítko **OK**. Pokud již v databázi klíčů máte osobní certifikát, otevře se okno se žádostí, zda chcete nastavit klíč, který přidáváte jako výchozí klíč v databázi.
11. Klepněte na tlačítko **Ano** nebo **Ne**. Otevře se okno Zadat jmenovku.
12. Klepněte na tlačítko **OK**. Pole **Osobní certifikáty** zobrazuje štítek nového osobního certifikátu, který jste přidali.

z příkazového řádku,

Chcete-li přidat osobní certifikát do souboru databáze klíčů, použijte některý 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*
Uvádí plně kvalifikovaný název souboru osobního certifikátu.

-db *název_souboru*
Uvádí plně kvalifikovaný název souboru databáze klíčů CMS.

-pw *heslo*
Určuje heslo pro databázi klíčů CMS.

-format *ascii*
Určuje 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 ICC používá algoritmy ověřené dle standardu FIPS 140-2. Pokud se komponenta ICC neinicializuje v režimu FIPS, příkaz **runmqakm** se nezdaří.

Používáte-li kryptografický hardware, přečtěte si téma "Přijímání osobního certifikátu do hardwaru vašeho PKCS #11" na stránce 309.

ALW *Extrakce certifikátu CA z úložiště klíčů v systému AIX, Linux, and Windows*

Chcete-li extrahovat certifikát CA, postupujte podle této procedury.

Použití produktu strmqikm

Potřebujete-li spravovat certifikáty TLS způsobem, který vyhovuje standardu FIPS, použijte příkaz **runmqakm** . **strmqikm** (iKeyman) neposkytuje volbu vyhovující FIPS.

Na počítači, ze kterého chcete extrahovat certifikát CA, proveďte následující kroky:

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 **Certifikáty podepsaného** a vyberte certifikát, který chcete extrahovat.
9. Klepněte na tlačítko **Extrahovat**. Otevře se okno extrahování certifikátu do souboru.
10. Vyberte volbu **Datový typ** certifikátu, například **Base64-encoded dat ASCII** pro soubor s příponou `.arm` .
11. Zadejte název souboru certifikátu a umístění, do kterého chcete certifikát uložit, nebo klepněte na tlačítko **Procházet** a vyberte název a umístění.
12. Klepněte na tlačítko **OK**. Certifikát bude zapsán do souboru, který jste zadali.

z příkazového řádku,

Pomocí následujících příkazů extrahujte certifikát CA pomocí příkazu **runmqckm** nebo příkazu **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 úplná cesta k databázi 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 ICC používá algoritmy ověřené dle standardu FIPS 140-2. Pokud se komponenta ICC neinicializuje v režimu FIPS, příkaz **runmqakm** se nezdaří.

ALW *Extrahování veřejné části certifikátu s automatickým podpisem z úložiště klíčů v systému AIX, Linux, and Windows*

Uvedeným postupem extrahujte 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 FIPS.

Na počítači, ze kterého chcete extrahovat veřejnou část certifikátu podepsaného sebou samým, proveďte následující kroky:

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 **Osobní certifikáty** a vyberte certifikát.
9. Klepněte na tlačítko **Extrahovat certifikát**. Otevře se okno extrahování certifikátu do souboru.
10. Vyberte volbu **Datový typ** certifikátu, například **Base64-encoded dat ASCII** pro soubor s příponou `.arm` .
11. Zadejte název souboru certifikátu a umístění, do kterého chcete certifikát uložit, nebo klepněte na tlačítko **Procházet** a vyberte název a umístění.
12. Klepněte na tlačítko **OK**. Certifikát bude zapsán do souboru, který jste zadali. Všimněte si, že když extrahujete (spíše než export) certifikát, je zahrnuta pouze veřejná část certifikátu, takže heslo není požadováno.

z příkazového řádku,

Pomocí následujících příkazů extrahujte veřejnou část certifikátu s automatickým podpisem pomocí produktu **runmqckm** nebo **runmqakm**:

- Použití runmqckkm:

```
runmqckm -cert -extract -db filename -pw password -label label -target filename
         -format ascii
```

- Použití runmqakm:

```
runmqakm -cert -extract -db filename -pw password -label label
            -target filename -format ascii -fips
```

kde:

`-db` *filename*	je úplná cesta k databázi 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 ICC používá algoritmy ověřené dle 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 (svým 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 ve formátu ASCII (UTF-8) nebo v kódování binárních (DER), protože produkt IBM Global Secure Toolkit (GSKit) nepodporuje certifikáty s jinými typy kódování.

Použití produktu `strmqikm`

Potřebujete-li spravovat certifikáty TLS způsobem, který vyhovuje standardu FIPS, použijte příkaz **runmqakm** . **strmqikm** neposkytuje volbu vyhovující 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 některý 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*
Uvádí plně kvalifikovaný název souboru databáze klíčů CMS.

-pw *heslo*
Určuje heslo pro databázi klíčů CMS.

-label *popisek*
Uvádí jmenovku přiloženou k certifikátu.

-file *název_souboru*
Uvádí jméno souboru obsahujícího certifikát.

-format *ascii*
Určuje 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 ICC používá algoritmy ověřené dle 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 podle této procedury.

Použití produktu `strmqikm`

Potřebujete-li spravovat certifikáty TLS způsobem, který vyhovuje standardu FIPS, použijte příkaz **runmqakm** . **strmqikm** (iKeyman) neposkytuje volbu vyhovující FIPS.

Na počítači, ze kterého chcete exportovat osobní certifikát, proveďte následující kroky:

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 **Osobní certifikáty** a vyberte certifikát, který chcete exportovat.
9. Klepněte na tlačítko **Exportovat/Importovat**. Otevře se okno Export/Import klíče.
10. Vyberte volbu **Exportovat klíč**.
11. Vyberte volbu **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 extrahovat) certifikát, jsou zahrnuty jak veřejné, tak i soukromé části certifikátu. To je důvod, proč je exportovaný soubor chráněn heslem. Když extrahujete certifikát, je zahrnuta pouze veřejná část certifikátu, takže heslo není požadováno.
14. Do pole **Heslo** zadejte heslo a zadejte je znovu do pole **Potvrdit heslo** .
15. Klepněte na tlačítko **OK**. Certifikát bude exportován do souboru, který jste zadali.

z příkazového řádku,

Vyexportujte osobní certifikát pomocí příkazu **runmqckm** nebo příkazu **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 `silná` nebo `slabá`. Předvolba je `strong`.

`-fips`	určuje, že příkaz má být spuštěn v režimu FIPS. V režimu FIPS komponenta ICC používá algoritmy ověřené dle 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 úplná cesta 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 celý platný řetězec certifikátu CA do souboru databáze klíčů (viz "Přidání certifikátu CA nebo veřejné části certifikátu podepsaného (svým držitelem) do úložiště klíčů v systému AIX, Linux, and Windows" na stránce 297).

Soubory PKCS #12 by měly být považovány za dočasné a odstraněné po použití.

Použití produktu `strmqikm`

Potřebujete-li spravovat certifikáty TLS způsobem, který je kompatibilní se standardem FIPS-, použijte příkaz **runmqakm** . **strmqikm** neposkytuje volbu vyhovující FIPS.

Na počítači, na který chcete importovat osobní certifikát, proveďte následující kroky:

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 **Osobní certifikáty**.
9. Pokud v zobrazení Osobní certifikáty existují certifikáty, proveďte následující kroky:
   a. Klepněte na tlačítko **Exportovat/Importovat**. Zobrazí se okno Export/Import klíče.
   b. Vyberte volbu **Importovat klíč**.
10. Pokud v zobrazení Osobní certifikáty nejsou žádné certifikáty, klepněte na tlačítko **Importovat**.
11. Vyberte volbu **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, které jste použili při exportu certifikátu.
15. Klepněte na tlačítko **OK**. Zobrazí se okno Změnit popisky. Můžete změnit jmenovky importovaných certifikátů, pokud již v cílové databázi klíčů již existuje certifikát se stejným popiskem. Změna návěští certifikátů nemá žádný vliv na ověření platnosti řetězu certifikátů. Chcete-li přiřadit certifikát

k určitému správci front nebo IBM MQ MQI client, IBM MQ použije buď hodnotu atributu **CERTLABL** , pokud je nastavena, nebo výchozí `ibmwebspheremq` s připojeným jménem správce front nebo přihlašovacího ID uživatele IBM MQ MQI client , vše malými písmeny. Podrobnosti najdete v tématu Digitální certifikáty certifikátu .

16. Chcete-li změnit popisek, vyberte požadovaný popisek ze seznamu **Vybrat popisek, který se má změnit** . Popisek popisku se zkopíruje do vstupního pole **Zadejte nový popisek** . Nahraďte text popisku novým popiskem a klepněte na tlačítko **Použít**.
17. Text ve vstupním poli **Zadat nový popisek** bude zkopírován zpět do pole **Vybrat štítek ke změně** a nahradí původně vybraný popisek a znovu označí příslušný certifikát.
18. Po změně všech jmenovek, které je třeba změnit, klepněte na tlačítko **OK**. Okno Změnit jmenovky se zavře a původní okno produktu IBM Key Management se znovu objeví s poli **Osobní certifikáty** a **Certifikáty podepsaného** s správně označenými certifikáty.
19. Certifikát je importován do databáze cílových 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 plně kvalifikovaný 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 má být importován ze zdrojové databáze klíčů.
`-new_label` *label*	je popisek, který bude certifikát přiřazen v cílové databázi. Vynecháte-li volbu `-new_label` , použije se výchozí hodnota pro použití stejné volby jako volba `-label` .
`-fips`	určuje, že příkaz má být spuštěn v režimu FIPS. V režimu FIPS komponenta ICC používá algoritmy ověřené dle standardu FIPS 140-2. Pokud se komponenta ICC neinicializuje v režimu FIPS, příkaz **runmqakm** se nezdaří.

Produkt **runmqckm** neposkytuje příkaz pro přímé změny popisků certifikátů. Chcete-li změnit jmenovku certifikátu, postupujte takto:

1. Exportujte certifikát do souboru PKCS #12 pomocí příkazu **-cert -export** . Uveďte existující jmenovku certifikátu pro volbu `-label` .
2. Odstraňte stávající kopii certifikátu z původní databáze klíčů pomocí příkazu **-cert -delete** .

3. Importujte certifikát ze souboru PKCS #12 pomocí příkazu **-cert -import** . Uveďte starý popisek pro volbu `-label` a požadovaný nový popisek pro volbu `-new_label` . Certifikát bude importován zpět do databáze klíčů s požadovaným popiskem.

ALW *Importování osobního certifikátu ze souboru Microsoft.pfx*

Postupujte podle této procedury pro import ze souboru Microsoft.pfx na systému AIX, Linux, and Windows.

Soubor .pfx může obsahovat dvě certifikáty vztahující se ke stejnému klíči. Jeden je osobní nebo organizační certifikát (obsahující veřejný i soukromý klíč). Druhým je certifikát CA (podepisujícího subjektu) (obsahuje pouze veřejný klíč). Tyto certifikáty nemohou existovat společně ve stejném souboru databáze klíčů CMS, takže lze importovat pouze jeden z nich. Také "popisný název" nebo štítek jsou připojeny pouze k certifikátu podepisujícího subjektu.

Osobní certifikát je identifikován systémem generovaným jedinečným identifikátorem uživatele (UUID). Tento oddíl zobrazuje import osobního certifikátu ze souboru pfx, zatímco jej opatřujete popiskem s popisným názvem, který byl dříve přiřazen k certifikátu CA (podepisujícího subjektu). Vydávání certifikátů CA (podepisujících subjektů) by již mělo být přidáno do cílové databáze klíčů. Všimněte si, že soubory PKCS#12 by měly být považovány za dočasné a odstraněné po použití.

Chcete-li importovat osobní certifikát ze zdrojové databáze klíčů pfx, proveďte následující kroky:

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 zálohování 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 označující, že soubor je otevřený a připravený.
6. Ze seznamu vyberte položku **Certifikáty podepsaného** . "Přátelské jméno" požadovaného certifikátu se zobrazí jako štítek v panelu Certifikáty podepsaného.
7. Vyberte položku štítku a klepnutím na tlačítko **Odstranit** odeberte certifikát podepsaného. Zobrazí se okno Potvrdit.
8. Klepněte na tlačítko **Ano**. Vybraný popisek se již nebude zobrazovat na panelu Certifikáty podepsaného.
9. Zopakujte kroky 6, 7 a 8 pro všechny certifikáty podepisujících subjektů.
10. V nabídce **Soubor databáze klíčů** klepněte na volbu **Otevřít**. Zobrazí se okno Otevřít.
11. Vyberte cílovou databázi CMS databáze, 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 označující, že soubor je otevřený a připravený.
13. Vyberte položku **Osobní certifikáty** ze seznamu.
14. Pokud v zobrazení Osobní certifikáty existují certifikáty, proveďte následující kroky:
    a. Klepněte na tlačítko **Exportovat/Importovat klíč**. Zobrazí se okno Export/Import klíče.
    b. Vyberte volbu **Importovat** z nabídky Vybrat typ akce.
15. Pokud v zobrazení Osobní certifikáty nejsou žádné certifikáty, klepněte na tlačítko **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 podepisujícího subjektu. Klepněte na tlačítko **OK**.
19. Zobrazí se okno Změnit popisky (protože by měl být k dispozici pouze jediný certifikát pro import). Návěští certifikátu by mělo být UUID, které má formát `xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx`.
20. Chcete-li změnit jmenovku, vyberte z panelu **Vyberte popisek, který se má změnit:** , vyberte klíč UUID. 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 `ibmwebspheremq` s připojeným jménem správce front nebo ID přihlášení uživatele IBM MQ MQI client , vše malými písmeny. Podrobnosti najdete v tématu Digitální certifikáty certifikátu .
21. Klepněte na tlačítko **OK**. Okno Změnit popisky je nyní odebráno a původní okno Správa klíčů produktu IBM se znovu objeví s osobními certifikáty a panely Certifikáty podepsaného, které byly aktualizovány se správně označeným osobním certifikátem.
22. Osobní certifikát pfx je nyní importován do databáze (cíle).

Není možné změnit jmenovku 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 plně kvalifikovaný 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 má být importován ze zdrojové databáze klíčů.
`-new_label` *label*	je popisek, který bude certifikát přiřazen v cílové databázi. Vynecháte-li volbu `-new_label` , použije se výchozí hodnota pro použití stejné volby jako volba `-label` .
`-fips`	určuje, že příkaz má být spuštěn v režimu FIPS. V režimu FIPS komponenta ICC používá algoritmy ověřené dle 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 přímé změny popisků certifikátů. Chcete-li změnit jmenovku certifikátu, postupujte takto:

1. Exportujte certifikát do souboru PKCS #12 pomocí příkazu **-cert -export** . Uveďte existující jmenovku certifikátu pro volbu `-label` .
2. Odstraňte stávající kopii certifikátu z původní databáze klíčů pomocí příkazu **-cert -delete** .
3. Importujte certifikát ze souboru PKCS #12 pomocí příkazu **-cert -import** . Uveďte 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 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. Z rozevíracího seznamu vyberte **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 299).
11. S vybraným certifikátem klepněte na tlačítko **Odstranit**. Otevře se okno Potvrdit.
12. Klepněte na tlačítko **Ano**. Pole **Osobní certifikáty** již nezobrazuje štítek certifikátu, který jste odstranili.

z příkazového řádku,

Pomocí následujících příkazů můžete odstranit certifikát pomocí příkazu **runmqckm** nebo příkazu **runmqakm** :

Použití runmqckkm:

```
runmqckm -cert -delete -db filename -pw password -label label
```

Použití runmqakm:

```
runmqakm -cert -delete -db filename -pw password -label label -fips
```

kde:

`-db` *filename*	je plně kvalifikovaný název souboru databáze klíčů CMS.
`-pw` *password*	je heslo pro databázi klíčů CMS.
`-label` *label*	je jmenovka přiložená k osobnímu certifikátu.
`-fips`	určuje, že příkaz má být spuštěn v režimu FIPS. V režimu FIPS komponenta ICC používá algoritmy ověřené dle standardu FIPS 140-2. Pokud se komponenta ICC neinicializuje v režimu FIPS, příkaz **runmqakm** se nezdaří.

ALW *Generování silných hesel pro ochranu úložiště klíčů v systému AIX, Linux, and Windows*

Pomocí příkazu **runmqakm** (GSKCapiCmd) můžete generovat silná hesla pro ochranu pomocí úložiště klíčů.

Chcete-li vygenerovat silné heslo, můžete použít příkaz **runmqakm** s následujícími parametry:

```
runmqakm -random -create -length 14 -strong -fips
```

Při použití vygenerovaného hesla v parametru **-pw** v následujících příkazech pro administraci certifikátů vždy uzavřete heslo do dvojitých uvozovek. Na systémech AIX and Linux musíte také použít znak zpětného lomítka, abyste se vyhnuli následujícím znakům, pokud se objeví v řetězci hesla:

```
! \ " '
```

Při zadávání hesla v odezvě na výzvu z produktu **runmqckm**, **runmqakm** nebo GUI **strmqikm** není nutné, aby heslo ucitli nebo aby se z něj vytekli. Není to nutné, protože shell operačního systému nemá vliv na zadávání dat v těchto případech.

ALW *Konfigurace pro kryptografický hardware na systému AIX, Linux, and Windows*

Šifrovací hardware pro správce front nebo klienta můžete nakonfigurovat mnoha způsoby.

Šifrovací hardware pro správce front v systému AIX, Linux, and Windows lze konfigurovat pomocí jedné z následujících metod:

- Použijte příkaz ALTER QMGR MQSC s parametrem SSLCRYP, jak je popsáno v tématu ALTER QMGR.
- Použijte nástroj IBM MQ Explorer ke konfiguraci kryptografického hardwaru ve vašem systému AIX, Linux, and Windows . Další informace najdete v online nápovědě.

Šifrovací hardware pro klienta IBM MQ v systému AIX, Linux, and Windows můžete nakonfigurovat pomocí jedné z následujících metod:

- Nastavte proměnnou prostředí MQSSLCRYP. Povolené hodnoty pro vlastnost MQSSLCRYP jsou stejné jako u parametru SSLCRYP, jak je popsáno v tématu ALTER QMGR.

  Pokud použijete verzi parametru SSLCRYP GSK_PKCS11 , štítek tokenu PKCS #11 se musí shodovat s popiskem, se kterým jste nakonfigurovali hardware.
- Nastavte atribut SSLCryptographicHardware v sekci SSL konfiguračního souboru IBM MQ client . Povolené hodnoty jsou stejné jako u parametru SSLCRYP, jak je popsáno v tématu ALTER QMGR.

  Pokud použijete verzi parametru SSLCRYP GSK_PKCS11 , štítek tokenu PKCS #11 se musí shodovat s popiskem, se kterým jste nakonfigurovali hardware.
- Nastavte pole **CryptoHardware** ve struktuře voleb konfigurace SSL, MQSCO, na volání MQCONNX. Další informace viz Přehled pro MQSCO.

Upozornění: V 9.2.3 Při dodávání konfigurace kryptografického hardwaru prostřednictvím proměnné prostředí MQSSLCRYP nebo atributu **SSLCryptoHardware** byste měli chránit heslo před uložením. Další informace viz “Klienti IBM MQ používající kryptografický hardware” na stránce 555.

Pokud jste nakonfigurovali kryptografický hardware, který používá rozhraní PKCS #11 pomocí některé z těchto metod, musíte uložit osobní certifikát pro použití na vašich kanálech v souboru databáze klíčů pro šifrovací token, který jste nakonfigurovali. Tento popis je popsán v tématu “Správa certifikátů na hardwaru PKCS #11” na stránce 306.

ALW *Správa certifikátů na hardwaru PKCS #11*

Můžete spravovat digitální certifikáty na kryptografickém hardwaru, který podporuje rozhraní PKCS #11 .

Informace o této úloze

Musíte vytvořit databázi klíčů pro přípravu prostředí produktu IBM MQ , a to i v případě, že nechcete v něm ukládat certifikáty certifikační autority (CA), ale budou ukládat všechny své certifikáty na váš kryptografický hardware. Databáze klíčů je nezbytná, aby správce front odkazoval na své pole SSLKEYR nebo pro aplikaci klienta na odkaz v proměnné prostředí MQSSLKEYR. Tato databáze klíčů je také povinná, pokud vytváříte žádost o certifikát.

Databázi klíčů vytvoříte buď pomocí příkazového řádku, nebo pomocí uživatelského rozhraní produktu **strmqikm** (iKeyman).

Postup

Vytvořte databázi klíčů pomocí příkazového řádku.

1. Spusťte některý z následujících příkazů:

- Použití **runmqckm**:

```
runmqckm -keydb -create -db filename -pw password -type cms -stash
```

- Použití **runmqakm**:

```
runmqakm -keydb -create -db filename -pw password -type cms
-stash -fips -strong
```

kde:

-db *název_souboru*
Uvádí plně kvalifikovaný název souboru databáze klíčů CMS a musí mít příponu souboru `.kdb`.

-pw *heslo*
Určuje heslo pro databázi klíčů CMS.

-type *cms*
Uvádí typ databáze. (Pro IBM MQmusí být `cms`.)

-stash
Uloží heslo databáze klíčů do souboru.

-fips
určuje, že příkaz má být spuštěn v režimu FIPS. Při použití režimu FIPS komponenta ICC používá algoritmy, které jsou validovány FIPS 140-2. Pokud se komponenta ICC neinicializuje v režimu FIPS, příkaz **runmqakm** se nezdaří.

-silné
Kontroluje, zda zadané heslo splňuje minimální požadavky na odolnost hesla. Minimální požadavky na heslo jsou tyto:

- Heslo musí mít minimální délku 14 znaků.
- Heslo musí obsahovat minimálně jedno malé písmeno, jedno velké písmeno a jednu číslici nebo speciální znak. Mezi speciální znaky patří hvězdička (*), znak dolaru ($), symbol čísla (#) a znak procenta (%). Prostor je klasifikován jako speciální znak.
- Každý znak může v hesle nastat maximálně třikrát.
- Maximální počet dvou po sobě jdoucích znaků v hesle může být stejný.
- Všechny znaky jsou ve standardním tisknutelném znakové sadě ASCII, v rozsahu 0x20 - 0x7E.

Volitelně můžete vytvořit databázi klíčů pomocí uživatelského rozhraní produktu **strmqikm** (iKeyman).

2. V systémech AIX and Linux se přihlaste jako uživatel root. V systému 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 produktu IBM MQ .
   - Na systémech Windows je soubor vlastností zabezpečení Java umístěn v podadresáři `java\jre\lib\security` instalačního adresáře produktu IBM MQ .

   Pokud se v souboru dosud nenachází, 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 nabídku **Soubor databáze klíčů** > **Otevřít**.
6. Klepněte na volbu **Typ databáze klíčů** a vyberte volbu **PKCS11Direct**.
7. Do pole **Název souboru** zadejte název modulu správy kryptografického hardwaru, například `PKCS11_API.so`.

Používáte-li certifikáty nebo klíče uložené na šifrovacím hardwaru PKCS #11, uvědomte si, že **runmqckm** a **strmqikm** 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, neboť programy **strmqikm** a **runmqckm** jsou na těchto platformách 32bitové.

8. Do pole **Umístění** zadejte cestu:
   - V systémech AIX and Linux to může být například `/usr/lib/pksc11`.
   - V systému Windows můžete zadat název knihovny, například `cryptoki`.

   Klepněte na tlačítko **OK**. Otevře se okno Otevřít kryptografický token.
9. Vyberte popisek tokenu šifrovacího zařízení, který chcete použít k ukládání certifikátů.
10. Do pole **Heslo šifrovacího tokenu** zadejte heslo, které jste nastavili při konfiguraci kryptografického hardwaru.
11. Má-li váš kryptografický hardware kapacitu k ukládání certifikátů podepisujících subjektů požadovaných pro příjem nebo import osobního certifikátu, zrušte zaškrtnutí obou políček sekundární databáze klíčů a pokračujte krokem “15” na stránce 308.

    Pokud vyžadujete, aby sekundární databáze klíčů CMS byla držitelem certifikátů podepsaného, vyberte buď volbu **Otevřít existující soubor databáze sekundárních klíčů** , nebo volbu **Vytvořit nový soubor databáze sekundárního klíče**.
12. Do pole **Název souboru** zadejte název souboru. Toto pole již obsahuje text `key.kdb`. Pokud je váš název kmene `key`, ponechte toto pole nezměněné. Pokud jste uvedli jiný název souboru, nahraďte `key` svým kmenovým jménem. Nesmíte změnit příponu `.kdb` .
13. V poli **Umístění** zadejte cestu, například:
    - Pro správce front: `/var/mqm/qmgrs/QM1/ssl`
    - Pro IBM MQ MQI client: `/var/mqm/ssl`

    Klepněte na tlačítko **OK**. Otevře se okno Výzva k zadání hesla.
14. Zadejte heslo.

    Pokud jste v kroku “11” na stránce 308vybrali volbu **Otevřít existující databázový soubor sekundárního klíče** , zadejte do pole **Heslo** heslo.

    Pokud jste v kroku “11” na stránce 308vybrali volbu **Vytvořit nový soubor databáze sekundárního klíče** , proveďte následující dílčí kroky:

    a) Do pole **Heslo** zadejte heslo a zadejte je znovu do pole **Potvrdit heslo** .

    b) Vyberte **Stash heslo pro soubor**. Všimněte si, že pokud heslo nezamačujete, pokusy o spuštění kanálů TLS selžou, protože nemohou získat heslo požadované pro přístup k souboru databáze klíčů.

    c) Klepněte na tlačítko **OK**. Zobrazí se okno s potvrzením, že heslo je v souboru `key.sth` (pokud jste neuvedli jiný název kmene).
15. Klepněte na tlačítko **OK**.

    Zobrazí se rámec s obsahem databáze klíčů.

ALW *Požádání o osobní certifikát pro hardware PKCS #11*

Tento postup použijte buď pro správce front, nebo pro IBM MQ MQI client , abyste požádali o osobní certifikát pro váš kryptografický hardware.

Informace o této úloze

Tato úloha popisuje, jak používat uživatelské rozhraní produktu **strmqikm** k vyžádání osobního certifikátu. Pokud používáte rozhraní příkazového řádku, prohlédněte si téma “z příkazového řádku,” na stránce 291.

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 .

Názvy algoritmů digitálního podpisu SHA3WithRSA a SHA5WithRSA jsou zamítnuty, protože se jedná o zkrácený tvar SHA384WithRSA a SHA512WithRSA .

Postup

Chcete-li požádat o osobní certifikát z uživatelského rozhraní produktu **strmqikm** (iKeyman), postupujte takto:

1. Postupujte takto, abyste mohli pracovat s vaším kryptografickým hardwarem. Viz “Správa certifikátů na hardwaru PKCS #11” na stránce 306.
2. V nabídce **Vytvořit** klepněte na **Nový požadavek na certifikát**.

   Otevře se okno Vytvořit nový klíč a žádost o certifikát.
3. Do pole **Jmenovka klíče** zadejte jmenovku certifikátu.

   Jmenovka je buď hodnota atributu **CERTLABL** , je-li nastavena, nebo standardní `ibmwebspheremq` s připojeným jménem správce front nebo IBM MQ MQI client ID uživatele pro přihlášení, vše malými písmeny. Podrobnosti najdete v tématu Digitální certifikáty certifikátu .
4. Vyberte volbu **Velikost klíče** a **Algoritmus podpisu** , které požadujete.
5. Zadejte hodnoty do pole **Obecný název** a **Organizace**a vyberte volbu **Země**. U zbývajících volitelných polí buď přijměte výchozí hodnoty, nebo zadejte nové hodnoty nebo vyberte nové hodnoty.

   Všimněte si, že v poli **Organizační jednotka** můžete zadat pouze jeden název. Další informace o těchto polích naleznete v tématu “Rozlišující názvy” na stránce 11.
6. Do pole **Zadejte název souboru, do kterého chcete uložit žádost o certifikát** , buď přijměte výchozí `certreq.arm`, nebo zadejte novou hodnotu s úplnou cestou.
7. Klepněte na tlačítko **OK**.

   Otevře se okno Potvrzení.
8. Klepněte na tlačítko **OK**.

   V seznamu **Požadavky na osobní certifikáty** je zobrazen popisek nové žádosti o osobní certifikát, kterou jste vytvořili. Požadavek na certifikát je uložen v souboru, který jste zvolili v kroku “6” na stránce 309.
9. Vyžádejte si nový osobní certifikát odesláním souboru certifikační autoritě (CA) nebo zkopírováním souboru do formuláře požadavku na webovém serveru pro CA.

ALW *Přijímání osobního certifikátu do hardwaru vašeho PKCS #11*

Tento postup použijte buď pro správce front, nebo pro produkt IBM MQ MQI client , který obdrží osobní certifikát pro váš kryptografický hardware.

Než začnete

Přidejte certifikát CA od CA, který podepsal osobní certifikát. Přidejte ji buď do kryptografického hardwaru, nebo do sekundární databáze klíčů CMS. Tuto akci proveďte před tím, než obdržíte podepsaný certifikát do kryptografického hardwaru. Chcete-li přidat certifikát CA do svazku klíčů, postupujte podle pokynů v části “Přidání certifikátu CA nebo veřejné části certifikátu podepsaného (svým držitelem) do úložiště klíčů v systému AIX, Linux, and Windows” na stránce 297.

Procedura

- Chcete-li obdržet osobní certifikát pomocí uživatelského rozhraní produktu **strmqikm** (iKeyman), postupujte takto:

  a) Postupujte takto, abyste mohli pracovat s vaším kryptografickým hardwarem. Viz “Správa certifikátů na hardwaru PKCS #11” na stránce 306.

  b) Klepněte na tlačítko **Přijmout**. Otevře se okno Přijmout certifikát ze souboru.

c) Zadejte název souboru certifikátu a umístění pro nový osobní certifikát, nebo klepněte na tlačítko **Procházet** a vyberte název a umístění.

d) Klepněte na tlačítko **OK**. Pokud již v databázi klíčů máte osobní certifikát, otevře se okno s dotazem, zda chcete nastavit klíč, který přidáváte jako výchozí klíč v databázi.

e) Klepněte na tlačítko **Ano** nebo **Ne**. Otevře se okno Zadat jmenovku.

f) Klepněte na tlačítko **OK**. V seznamu **Osobní certifikáty** je zobrazen popisek nového osobního certifikátu, který jste přidali. Tento štítek je vytvořen přidáním štítku šifrovacího tokenu před popis, který jste zadali.

- Chcete-li obdržet osobní certifikát pomocí příkazu **runmqakm** (GSKCapiCmd), proveďte následující kroky:

  a) Otevřete příkazové okno, které je nakonfigurované pro vaše prostředí.

  b) Přijmout 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*
  Uvádí plně kvalifikovaný název souboru, který obsahuje osobní certifikát.

  -šifrování *název_modulu*
  Uvádí plně kvalifikovaný název knihovny PKCS #11 dodané s kryptografickým hardwarem.

  -tokenlabel *hardwareční_token*
  Uvádí jmenovku tokenu šifrovacího zařízení PKCS #11 .

  -pw *heslo_hardwaru_hardwaru*
  Určuje heslo pro přístup k kryptografickému hardwaru.

  -format *formát_certifikátu*
  Určuje formát certifikátu. Hodnota může být `ascii` pro ASCII kódované formátem Base64 nebo `binary` pro binární data DER. Předvolba je ASCII.

  -fips
  určuje, že příkaz má být spuštěn v režimu FIPS. Při použití režimu FIPS komponenta ICC používá algoritmy, které jsou validovány FIPS 140-2. Pokud se komponenta ICC neinicializuje v režimu FIPS, příkaz **runmqakm** se nezdaří.

  -secondaryDB *název_souboru*
  Uvádí plně kvalifikovaný název souboru databáze klíčů CMS.

  -secondaryDBpw *heslo*
  Určuje heslo pro databázi klíčů CMS.

MQ Appliance Práce s SSL/TLS v IBM MQ Appliance

IBM MQ Appliance má podporu TLS (Transport Layer Security).

IBM MQ Appliance má odlišné příkazy pro správu certifikátů. Podrobné informace o správě certifikátů viz dokumentace produktu IBM MQ Appliance , správa certifikátů TLS .

z/OS Práce s SSL/TLS v z/OS

Tyto informace popisují, jak jste nastavili a pracují s TLS (Transport Layer Security) na serveru z/OS.

Každé téma obsahuje příklady provedení jednotlivých úloh pomocí produktu RACF. Podobné úlohy můžete provádět pomocí jiných externích správců zabezpečení.

V systému z/OSje třeba nastavit také počet dílčích úloh serveru, které každý správce front používá pro zpracování volání TLS, jak je popsáno v tématu “Nastavení parametru SSLTASKS v systému z/OS” na stránce 311.

Podpora TLS z/OS je integrální součástí operačního systému a je známá jako *System SSL*. System SSL je součástí základního prvku Cryptographic Services Base produktu z/OS. Základní členové produktu Cryptographic Services Base jsou nainstalováni v adresáři *pdsname*. Sada datových sad SEIALNKE (rozdělená datová sada (PDS)). Při instalaci zabezpečení SSL systému se ujistěte, že jste zvolili příslušné volby pro poskytnutí vámi vyžadování CipherSpecs .

z/OS Další požadavky na ID uživatele pro TLS v systému z/OS

Tyto informace popisují další požadavky, které vaše ID uživatele potřebuje pro nastavení a práci s TLS v systému z/OS.

Ujistěte se, že máte ve svém systému všechny vhodné aktualizace typu High Impact nebo Pervasive (HIPER).

Ujistěte se, že jste nastavili následující předpoklady:

- ID uživatele *ssidCHIN* je v produktu RACFsprávně definováno a že ID uživatele *ssidCHIN* má přístup pro čtení k následujícím profilům:
  - IRR.DIGTCERT.LIST
  - IRR.DIGTCERT.LISTRING

  Tyto proměnné jsou definovány ve třídě FACILITY RACF .
- ID uživatele *ssidCHIN* je vlastníkem svazku klíčů.
- Osobní certifikát správce front, pokud byl vytvořen příkazem RACDCERT, je vytvořen s ID uživatele pro typ certifikátu, který je také stejný jako ID uživatele *ssidCHIN* .
- Inicializátor kanálu je recyklován nebo je zadán příkaz **REFRESH SECURITY TYPE(SSL)** k výběru všech změn, které jste provedli v klíčovém kruhu.
- Procedura iniciátoru kanálu produktu IBM MQ má přístup k systémové knihovně běhového prostředí SSL *název_dsn*.SIEALNIKE prostřednictvím seznamu odkazů, LPA nebo příkazu STEPLIB DD. Tato knihovna musí být autorizovaná APF.
- ID uživatele, pod jehož oprávněním je spuštěn inicializátor kanálu, je nakonfigurováno pro použití produktu z/OS UNIX System Services (z/OS UNIX), jak je popsáno v dokumentaci Plánování z/OS UNIX System Services .

  Uživatelé, kteří nechtějí, aby inicializátor kanálu vyvolal z/OS UNIX za použití guest/default UID a segmentu OMVS, potřebuje pouze model nového segmentu OMVS na základě výchozího segmentu, protože inicializátor kanálu nevyžaduje žádná speciální oprávnění a není spuštěn v rámci UNIX jako superuživatel.

z/OS Nastavení parametru SSLTASKS v systému z/OS

Použijte příkaz ALTER QMGR k nastavení počtu podúloh serveru pro zpracování volání TLS

Chcete-li používat TLS kanály, ujistěte se, že existuje alespoň dvě podúlohy serveru nastavením parametru SSLTASKS pomocí příkazu ALTER QMGR. 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 kontrolována seznam CRL (Certificate Revocation List).

Je-li použita kontrola CRL, je v daném kanálu zadržen SSLTASK po dobu trvání této kontroly. Důvodem může být významná uplynulá doba, kdy je kontaktován relevantní server LDAP, protože každá SSLTASK je řídicí blok úloh z/OS .

Chcete-li změnit hodnotu atributu SSLTASKS, musíte restartovat inicializátor kanálu.

z/OS *Nastavení úložiště klíčů v systému z/OS*

Nastavte úložiště klíčů na obou koncích připojení. Přidružte každé úložiště klíčů ke svému správci front.

Připojení TLS vyžaduje *úložiště klíčů* na každém konci připojení. Každý správce front musí mít přístup k úložišti klíčů. Chcete-li přiřadit úložiště klíčů ke správci front, použijte parametr SSLKEYR v příkazu ALTER QMGR. Další informace viz “Úložiště klíčů SSL/TLS” na stránce 23.

V operačním systému z/OSjsou digitální certifikáty uloženy v *svazku klíčů* spravovaném externím správcem zabezpečení (ESM). Tyto digitální certifikáty mají štítky, které přidružují certifikát ke správci front. TLS používá tyto certifikáty pro účely autentizace. Všechny příklady, které následují za použití příkazů RACF . Pro ostatní programy ESM existují ekvivalentní příkazy.

V systému z/OSpoužívá produkt IBM MQ buď hodnotu atributu **CERTLABL** , pokud je nastavena, nebo výchozí `ibmWebSphereMQ` s připojeným názvem správce front. Podrobnosti najdete v tématu Digitální certifikáty certifikátu .

Název úložiště klíčů pro správce front je názvem svazku klíčů ve vaší databázi RACF . Název klíčového řetězce 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 pro vydání příkazu RACDCERT (viz *SecureWay Security Server RACF Command Language Reference* , kde získáte další podrobnosti).
2. Spusťte následující příkaz:

   ```
   RACDCERT ID( userid1 ) ADDRING( ring-name )
   ```

   kde:

   - *userid1* je ID uživatele adresního prostoru inicializátoru kanálu nebo ID uživatele, které bude vlastnit klíč svazku klíčů (je-li svazek klíčů sdílený).
   - *ring-name* je jméno, které chcete dát do svazku klíčů. Délka tohoto názvu může být až 237 znaků. V tomto jménu se rozlišují velká a malá písmena. Chcete-li se vyhnout problémům, zadejte velkými písmeny řetězec *ring-name* .

z/OS *Zpřístupnění certifikátů CA pro správce front v systému z/OS*

Po vytvoření svazku klíčů připojte k němu všechny příslušné certifikáty CA.

Máte-li v datové sadě certifikát CA, musíte nejprve přidat certifikát do databáze RACF pomocí následujícího příkazu:

```
RACDCERT ID( userid1 ) ADD( input-data-set-name ) WITHLABEL( 'My CA' )
```

Poté pro připojení certifikátu CA pro My CA ke svému svazku klíčů použijte tento příkaz:

```
RACDCERT ID(userid1)
CONNECT(CERTAUTH LABEL('My CA') RING(ring-name) USAGE(CERTAUTH))
```

kde *userid1* je buď ID uživatele iniciátoru kanálu, nebo vlastník sdíleného svazku klíčů.

Další informace o certifikátech CA najdete v tématu “digitální certifikáty” na stránce 9.

z/OS *Vyhledání úložiště klíčů pro správce front v systému z/OS*

Tuto proceduru použijte k získání umístění svazku klíčů správce front.

1. Zobrazte atributy správce front pomocí jednoho z následujících příkazů MQSC:

   ```
   DISPLAY QMGR ALL
   DISPLAY QMGR SSLKEYR
   ```

2. Prohlédněte si výstup příkazu pro umístění svazku klíčů.

z/OS *Určení umístění úložiště klíčů pro správce front v systému z/OS*

Chcete-li zadat umístění svazku klíčů správce front, nastavte atribut úložiště klíčů správce front pomocí příkazu ALTER QMGR MQSC.

Příklad:

```
ALTER QMGR SSLKEYR(CSQ1RING)
```

pokud je svazek klíčů vlastněný adresním prostorem inicializátoru kanálu, nebo:

```
ALTER QMGR SSLKEYR(userid1/CSQ1RING)
```

pokud se jedná o sdílený svazek klíčů, kde *userid1* je ID uživatele, který vlastní tento svazek klíčů.

z/OS *Udělením inicializátoru kanálu správná přístupová práva v systému z/OS*

Inicializátor kanálu (CHINIT) potřebuje přístup k úložišti klíčů a k určitým profilům zabezpečení.

Udělení přístupu CHINIT ke čtení úložiště klíčů

Je-li úložiště klíčů vlastněno ID uživatele CHINIT, tento ID uživatele potřebuje přístup pro čtení k IRR.DIGTCERT.LISTRING profilu ve třídě FACILITY a v opačném případě aktualizujte přístup. Udělte přístup pomocí příkazu PERMIT s možností ACCESS (UPDATE) nebo ACCESS (READ) podle potřeby:

```
PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID( userid ) ACCESS(UPDATE)
```

, kde *id_uživatele* je ID uživatele adresního prostoru inicializátoru kanálu.

Udělení přístupu pro čtení CHINIT k příslušným profilům CSF*

Pro použití hardwarové podpory poskytované prostřednictvím rozhraní ICSF (Integrated Cryptographic Service Facility) zajistěte, aby vaše ID uživatele CHINIT mělo 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

ID uživatele CHINIT může také potřebovat přístup pro čtení k jiným profilům CSF*. Pokud například používáte specifikaci šifry ECDHE_RSA_AES_256_GCM_SHA384 , bude mít vaše ID uživatele CHINIT také přístup pro čtení k následujícím profilům CSF*:

- CSF1DVK
- CSF1GAV
- CSF1GKP
- CSF1SKE
- CSF1TRC

- CSF1TRD

Další informace naleznete v tématu Požadavky na prostředky RACF CSFSERV.

Pokud jsou vaše klíče certifikátů uloženy ve službě ICSF a vaše instalace zavedla řízení přístupu přes klíče uložené 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 *id_uživatele* je ID uživatele adresního prostoru inicializátoru kanálu.

Použití programu ICSF (Integrated Cryptographic Service Facility)

Inicializátor kanálu může použít službu ICSF k vygenerování náhodného čísla při zavedení algoritmu ochrany heslem pro zamaskování hesel procházejících přes kanály klienta, pokud se TLS nepoužívá.

Další informace naleznete v tématu “Použití programu ICSF (Integrated Cryptographic Service Facility)” na stránce 258 .

z/OS *Když změny certifikátů nebo úložiště klíčů vstoupí v platnost v z/OS*

Změny se projeví po spuštění inicializátoru kanálu nebo při aktualizaci úložiště.

Konkrétně změny certifikátů v souboru svazku klíčů a atributu úložiště klíčů se projeví při jedné z následujících akcí:

- Při spuštění nebo restartování inicializátoru kanálu.
- Když je vydán příkaz REFRESH SECURITY TYPE (SSL) k aktualizaci obsahu úložiště klíčů.

z/OS *Vytvoření osobního certifikátu podepsaného sebou samým na serveru z/OS*

Pomocí této procedury vytvoříte osobní certifikát podepsaný sám sebou samým.

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 svému 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 vlastník sdíleného svazku klíčů.
- *userid2* je ID uživatele přidružené k certifikátu a musí se jednat o ID uživatele adresního prostoru inicializátoru kanálu.

  userid1 a *userid2* mohou být stejné ID.
- Parametr *název-svazku* je název, který jste přiřadili svazku klíčů v produktu “Nastavení úložiště klíčů v systému z/OS” na stránce 312.
- *název-návěští* musí být buď hodnota atributu IBM MQ **CERTLABL** , je-li nastavena, nebo výchozí `ibmWebSphereMQ` s připojeným názvem správce front. Podrobnosti najdete v tématu Digitální certifikáty certifikátu .

z/OS Požádání o osobní certifikát v systému z/OS

Použijte pro osobní certifikát pomocí produktu RACF.

Chcete-li požádat o osobní certifikát, použijte příkaz RACF takto:

1. Vytvořte osobní certifikát podepsaný sám sebou, jako v produktu “Vytvoření osobního certifikátu podepsaného sebou samým na serveru z/OS” na stránce 314. Tento certifikát poskytuje požadavek s hodnotami atributu pro rozlišující název.
2. Vytvořte požadavek certifikátu PKCS #10 Base64-encoded napsaný 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 to být ID uživatele adresního prostoru inicializátoru kanálu
   - *label_name* je jmenovka použitá při vytváření certifikátu podepsaného sebou samým

   Podrobnosti viz “Digitální certifikáty certifikátu, základní informace o požadavcích” na stránce 24.
3. Chcete-li požádat o nový osobní certifikát, odešlete datovou sadu certifikační autoritě (CA).
4. Když je podepsaný certifikát vrácen certifikační autoritou, přidejte certifikát zpět do databáze RACF pomocí původní jmenovky, jak je popsáno v “Přidání osobních certifikátů do úložiště klíčů v systému z/OS” na stránce 316.

z/OS Vytvoření osobního certifikátu podepsaného RACF

Produkt RACF může fungovat jako certifikační autorita a vydává svůj vlastní certifikát CA.

Tento oddíl používá termín *certifikát podepisujícího subjektu* k označení certifikátu CA vydaného produktem RACF.

Soukromý klíč pro certifikát podepsaného musí být v databázi RACF před tím, než provedete následující proceduru:

1. Pomocí následujícího příkazu vygenerujte osobní certifikát podepsaný pomocí produktu RACFs použitím certifikátu podepsaného obsaženého ve vaší 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 svému 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 vlastník sdíleného svazku klíčů.
- *userid2* je ID uživatele přidružené k certifikátu a musí se jednat o ID uživatele adresního prostoru inicializátoru kanálu.

  userid1 a *userid2* mohou být stejné ID.

- Parametr *název-svazku* je název, který jste přiřadili svazku klíčů v produktu “Nastavení úložiště klíčů v systému z/OS” na stránce 312.
- *název-návěští* musí být buď hodnota atributu IBM MQ **CERTLABL** , je-li nastavena, nebo výchozí `ibmWebSphereMQ` s připojeným názvem správce front nebo skupiny sdílení front. Podrobnosti najdete v tématu Digitální certifikáty certifikátu .
- *signer-label* je popisek vašeho vlastního certifikátu podepisujícího subjektu.

z/OS *Přidání osobních certifikátů do úložiště klíčů v systému z/OS*

Tento postup slouží k přidání nebo importu osobního certifikátu do svazku klíčů.

Poté, co vám certifikační autorita odešle nový osobní certifikát, přidejte jej do svazku klíčů pomocí následující procedury:

1. Přidejte certifikát do databáze produktu RACF pomocí následujícího příkazu:

```
RACDCERT ID( userid2 ) ADD( input-data-set-name ) WITHLABEL(' label-name ')
```

2. Připojte certifikát ke svému 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 vlastník sdíleného svazku klíčů.
- *userid2* je ID uživatele přidružené k certifikátu a musí se jednat o ID uživatele adresního prostoru inicializátoru kanálu.
- Parametr *název-svazku* je název, který jste přiřadili svazku klíčů v produktu “Nastavení úložiště klíčů v systému z/OS” na stránce 312.
- *název-vstupní-datové-sady* je název datové sady, která obsahuje podepsaný certifikát CA. Datová sada musí být katalogizována a nesmí se jednat o rozdělenou datovou sadu (PDS) nebo o člen rozdělené datové sady (PDS). Formát záznamu (RECFM), který očekává RACDCERT, je VB. RACDCERT dynamicky přiděluje a otevře datovou sadu a přečte certifikát z něj jako binární data.
- *název-popisku* je název popisku, který byl použit při vytvoření původní žádosti. Musí to být buď hodnota atributu IBM MQ **CERTLABL** , je-li nastavena, nebo výchozí `ibmWebSphereMQ` s připojeným názvem správce front nebo skupiny sdílení front. Podrobnosti najdete v tématu Digitální certifikáty certifikátu .

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 tento 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-návěští* je jmenovka certifikátu, který chcete extrahovat.
- *název-výstupní-datové-sady* je datová sada, do které je certifikát umístěn.
- CERTB64 je certifikát X.509 kódovaný pomocí DER, který je ve formátu Base64 . Můžete zvolit alternativní formát, například:

  CERTDER
  certifikát kódovaný pomocí DER X.509 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*

Odstranění osobního certifikátu pomocí příkazu RACDCERT.

Před odstraněním osobního certifikátu můžete chtít uložit jeho kopii. Chcete-li zkopírovat svůj osobní certifikát do datové sady před jejím odstraněním, postupujte podle pokynů v části "Export osobního certifikátu z úložiště klíčů v systému z/OS" na stránce 316. Pak použijte následující příkaz k odstranění osobního certifikátu:

```
RACDCERT ID( userid2 ) DELETE(LABEL(' label-name '))
```

kde:

- *userid2* je ID uživatele, pod kterým byl certifikát přidán do svazku klíčů.
- *název-návěští* je jméno certifikátu, který chcete vymazat.

z/OS *Přejmenování osobního certifikátu v úložišti klíčů v systému z/OS*

Přejmenujte certifikát pomocí příkazu RACDCERT.

Pokud nechcete, aby byl nalezen certifikát s určitým popiskem, ale nechcete jej odstranit, můžete jej přejmenovat dočasně 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.
- Parametr *název-návěští* 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*

IBM MQ může použít ID uživatele přidružené k certifikátu RACF jako ID uživatele kanálu. Přidružte ID uživatele k certifikátu tak, že jej nainstalujete pod toto ID uživatele, nebo pomocí filtru názvu certifikátu.

Metoda popsaná v tomto tématu představuje alternativu k metodě pro přidružení ID uživatele k digitálnímu certifikátu, který používá záznamy ověřování kanálu. Další informace o záznamech ověření kanálu viz "Záznamy ověření kanálu" na stránce 47.

Když entita na jednom konci kanálu TLS obdrží certifikát od vzdáleného připojení, dotáže se RACF , zda existuje ID uživatele přidružené k tomuto certifikátu. Entita používá toto ID uživatele jako ID uživatele kanálu. Pokud k certifikátu není přidruženo žádné ID uživatele, bude entita používat ID uživatele, pod kterým je spuštěn inicializátor kanálu.

Přidružte ID uživatele k certifikátu jedním z následujících způsobů:

- Nainstalujte tento certifikát do databáze produktu 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 316.
- Použijte CNF (Certificate Name Filter) k mapování rozlišujícího názvu subjektu nebo vydavatele certifikátu na ID uživatele, jak je popsáno v "Nastavení filtru názvů certifikátů v systému z/OS" na stránce 318.

z/OS *Nastavení filtru názvů certifikátů v systému z/OS*

Pomocí příkazu RACDCERT můžete definovat filtr názvů certifikátů (CNF), který mapuje rozlišující název na ID uživatele.

Chcete-li nastavit CNF, proveďte následující kroky.

1. Povolte funkce CNF pomocí následujícího příkazu. K provedení této akce je zapotřebí 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:

   - DN subjektu má organizaci `IBM` a zemi s UK.
   - DN vydavatele má organizaci `ExampleCA` a lokalitou `Internet`.

3. Aktualizujte mapování CNF:

   ```
   SETROPTS RACLIST(DIGTNMAP) REFRESH
   ```

Poznámka:

1. Je-li skutečný certifikát uložen v databázi RACF , použije se ID uživatele, pod kterým je nainstalován, v preferovaném ID uživatele, který je přidružen k jakémukoli CNF. Není-li certifikát uložen v databázi RACF , použije se ID uživatele přidružené k nejspecifičtěji shodným CNF. Shoduje se s rozlišujícím názvem subjektu, které jsou považovány za specifičtější, než odpovídá rozlišujícímu názvu DN.
2. Změny do CNFs se nepoužijí, dokud neobnovíte mapování CNF.
3. DN se shoduje s filtrem DN v CNF pouze, pokud je filtr DN identický s *nejméně významnou částí* DN. Nejméně významná část DN se skládá z atributů, které jsou obvykle uvedeny na nejsprávnějším konci DN, ale které se objevují na začátku certifikátu.

   Vezměme si například příkaz SDNFILTER `'O=IBM.C=UK'`. Rozlišovací jméno subjektu `'CN=QM1.O=IBM.C=UK'` odpovídá tomuto filtru, ale rozlišující název subjektu `'CN=QM1.O=IBM.L=Hursley.C=UK'` neodpovídá tomuto filtru.

   Nejméně významná část některých certifikátů může obsahovat pole, která se neshodují s filtrem DN. Zvažte vyloučení těchto certifikátů uvedením vzoru DN v šabloně SSLPEER v příkazu DEFINE CHANNEL.
4. Pokud je nejspecifičtější odpovídající CNF definováno jako NOTRUST do RACF , entita používá ID uživatele, pod kterým je spuštěn inicializátor kanálu.
5. RACF používá znak `'.'` jako oddělovač. IBM MQ používá buď čárku, nebo středník.

Můžete definovat CNF, aby se zajistilo, 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 souboru svazku klíčů přidruženém k entitě definujte CNF s parametrem IDNFILTER, který přesně odpovídá rozlišujícímu názvu DN daného certifikátu CA. Tím je zajištěno, že všechny certifikáty, které může účetní jednotka použít, se budou shodovat alespoň s jedním z těchto CNFs. Důvodem je to, že všechny tyto certifikáty musí být buď připojeny ke svazku klíčů přidruženému k entitě, nebo musí být vydáno CA, pro který je certifikát připojen k svazku klíčů přidruženému k entitě.

Další informace o příkazech, které používáte k manipulaci s CNFs, naleznete v příručce *SecureWay Security Server RACF Security Administrator's Guide* .

z/OS *Definování kanálu odesílatele a přenosové fronty na QMA v systému z/OS*

Chcete-li nastavit vyžadované objekty, použijte příkazy **DEFINE CHANNEL** a **DEFINE QLOCAL** .

Postup

U správce QMA zadejte příkazy jako následující příklad:

```
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 odesílatele TO.QMBa vytvoří se přenosová fronta QMB.

z/OS *Definování přijímacího kanálu na QMB v systému z/OS*

Chcete-li nastavit požadovaný objekt, použijte příkaz **DEFINE CHANNEL** .

Postup

V QMB zadejte příkaz jako následující příklad:

```
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 vytvořeno.

z/OS *Spouštění kanálu odesílatele v QMA v systému z/OS*

Je-li to nezbytné, spusťte program listener a obnovte zabezpečení. Poté spusťte kanál pomocí příkazu **START CHANNEL** .

Postup

1. Volitelné: Pokud jste tak dosud neučinili, spusťte program modulu listener na QMB.

   Program modulu listener naslouchá příchozím požadavkům na síť a spouští přijímací kanál, když je potřeba. Informace o tom, jak spustit modul listener, najdete v tématu Spuštění modulu listener kanálu.
2. Volitelné: Pokud již byly spuštěny žádné kanály SSL/TLS, zadejte příkaz `REFRESH SECURITY TYPE(SSL)`.

   Tím je zajištěno, že všechny změny provedené v úložišti klíčů jsou dostupné.
3. Spusťte kanál na QMA pomocí příkazu `START CHANNEL(TO.QMB)`.

Výsledky

Kanál odesílatele je spuštěn.

z/OS *Výměna certifikátů s automatickým podpisem na z/OS*

Vyměňte certifikáty, které jste předtím extrahovali. Používáte-li protokol FTP, použijte správný formát.

Postup

Přeneste CA část certifikátu QM1 do systému QM2 a opačně, například pomocí FTP.

Pokud přenášejí certifikáty pomocí protokolu FTP, musíte tak učinit ve správném formátu.

Přeneste následující typy certifikátů ve formátu *binary* :

- Binární X.509 kódovaný pomocí DER
- PKCS #7 (certifikáty CA)
- PKCS #12 (osobní certifikáty)

Přeneste následující typy certifikátů ve formátu ASCII:

- PEM (ochrana soukromí-rozšířená pošta)
- Base64 kódováno X.509

z/OS *Definování kanálu odesílatele a přenosové fronty v systému QM1 v systému z/OS*

Chcete-li nastavit vyžadované objekty, použijte příkazy **DEFINE CHANNEL** a **DEFINE QLOCAL** .

Postup

V systému QM1zadejte příkazy jako následující příklad:

```
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)
```

Hodnota CipherSpecs na každém konci kanálu musí být stejná.

Pouze parametr SSLCIPH je povinný, pokud chcete, aby kanál používal TLS. Informace o povolených hodnotách pro parametr SSLCIPH naleznete v příručce “CipherSpecs a CipherSuites v produktu IBM MQ” na stránce 38 .

Výsledky

Odesílací kanál QM1.TO.QM2, a přenosová fronta QM2, se vytvoří.

z/OS *Definování přijímacího kanálu na systému QM2 v systému z/OS*

Chcete-li nastavit požadovaný objekt, použijte příkaz **DEFINE CHANNEL** .

Postup

V systému QM2zadejte příkaz podobný tomuto 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 odesílacího kanálu, který jste definovali v produktu “Definování kanálu odesílatele a přenosové fronty v systému QM1 v systému z/OS” na stránce 320, a použít stejnou CipherSpec.

z/OS *Spouštění kanálu odesílatele v systému QM1 v systému z/OS*

Je-li to nezbytné, spusťte program listener a obnovte zabezpečení. Poté spusťte kanál pomocí příkazu **START CHANNEL** .

Postup

1. Volitelné: Pokud jste tak dosud neučinili, spusťte program modulu listener na systému QM2.

   Program modulu listener naslouchá příchozím požadavkům na síť a spouští přijímací kanál, když je potřeba. Informace o tom, jak spustit modul listener, najdete v tématu Spuštění modulu listener kanálu .

2. Volitelné: Pokud již byly některé kanály SSL/TLS spuštěny dříve, zadejte příkaz REFRESH SECURITY TYPE (SSL).

   Tím je zajištěno, že všechny změny provedené v úložišti klíčů jsou dostupné.
3. V systému QM1spusťte kanál pomocí příkazu `START CHANNEL(QM1.TO.QM2)`.

Výsledky

Kanál odesílatele 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

Na správci QMA zadejte tento příkaz:

```
REFRESH SECURITY TYPE(SSL)
```

Tím je zajištěno, že všechny změny provedené v úložišti klíčů jsou dostupné.

z/OS *Povolení anonymních připojení na přijímacím kanálu v systému z/OS*

Použijte příkaz **ALTER CHANNEL** , abyste učinili ověření klienta SSL nebo TLS volitelné.

Postup

Na QMB zadejte tento příkaz:

```
ALTER CHANNEL(TO.QMB) CHLTYPE(RCVR) SSLCAUTH(OPTIONAL)
```

z/OS *Spouštění kanálu odesílatele v systému QM1 v systému z/OS*

V případě potřeby spusťte iniciátor kanálu, spusťte program modulu listener a obnovte zabezpečení. Poté spusťte kanál pomocí příkazu **START CHANNEL** .

Postup

1. Volitelné: Pokud jste tak dosud neučinili, spusťte iniciátor kanálu.
2. Volitelné: Pokud jste tak dosud neučinili, spusťte program modulu listener na systému QM2.

   Program modulu listener naslouchá příchozím požadavkům na síť a spouští přijímací kanál, když je potřeba. Informace o tom, jak spustit modul listener, najdete v tématu Spuštění modulu listener kanálu .
3. Volitelné: Pokud byl inicializátor kanálu již spuštěn nebo pokud již byly spuštěny nějaké kanály SSL/TLS, zadejte příkaz REFRESH SECURITY TYPE (SSL).

   Tím je zajištěno, že všechny změny provedené v úložišti klíčů jsou dostupné.
4. V systému QM1spusťte kanál pomocí příkazu `START CHANNEL(QM1.TO.QM2)`.

Výsledky

Kanál odesílatele je spuštěn.

z/OS *Spouštění kanálu odesílatele v QMA v systému z/OS*

V případě potřeby spusťte iniciátor kanálu, spusťte program modulu listener a obnovte zabezpečení. Poté spusťte kanál pomocí příkazu **START CHANNEL** .

Postup

1. Volitelné: Pokud jste tak dosud neučinili, spusťte iniciátor kanálu.
2. Volitelné: Pokud jste tak dosud neučinili, spusťte program modulu listener na QMB.

   Program modulu listener naslouchá příchozím požadavkům na síť a spouští přijímací kanál, když je potřeba. Informace o tom, jak spustit modul listener, najdete v tématu Spuštění modulu listener kanálu.
3. Volitelné: Pokud byl inicializátor kanálu již spuštěn nebo pokud již byly některé kanály SSL/TLS spuštěny dříve, zadejte příkaz `REFRESH SECURITY TYPE(SSL)`.

   Tím je zajištěno, že všechny změny provedené v úložišti klíčů jsou dostupné.
4. Spusťte kanál na QMA pomocí příkazu `START CHANNEL(TO.QMB)`.

Výsledky

Kanál odesílatele je spuštěn.

z/OS *Úprava délky klíče eliptické křivky na z/OS*

Jak upravíte proměnnou prostředí GSK_CLIENT_ECURVE_LIST pro nastavení seznamu eliptických křivek nebo podporovaných skupin, které jsou určeny klientem, jako řetězec sestávající z jedné nebo více 4znakových hodnot v preferovaném pořadí pro použití.

Důležité: Musíte použít opravu v z/OS APAR OA61783 , chcete-li povolit, aby některé eliptické křivky byly prováděny operačním systémem, když používáte TLS 1.0, TLS 1.1 a/nebo TLS 1.2 vyjednaná spojení.

Tuto proměnnou prostředí TLS můžete nastavit v kódu JCL pro spuštění inicializátoru kanálu pomocí příkazu CEEOPTS DD:

```
CEEOPTS DD DSN=<dataset-name>,DISP=SHR
```

V datové sadě, na kterou je odkazováno výše, uveďte seznam, který chcete použít, například:

```
ENVAR("GSK_CLIENT_ECURVE_LIST=002300240025")
```

Důležité: Nepoužívejte tento příkaz CEEOPTS s daty in-stream, protože tím zabráníte, aby proměnná prostředí byla nastavena pro všechny úlohy TLS pomocí tohoto příkazu.

Ujistěte se, že jste odkazovali na sekvenční datovou sadu nebo na člena datové sady rozdělené na oblasti, abyste umožnili, aby toto fungovalo, když používáte hodnotu SSLTASKS větší než jedna.

Můžete také použít analogový ekvivalent GSK_CLIENT_ECUROVE_LIST, který je GSK_SERVER_ALLOWED_KEX_ECURVES. Další informace najdete v tématu Omezení výměny klíčů eliptické křivky .

Kromě toho viz tabulka 5 v tématu Definice šifrovacích sad pro seznam platných specifikací 4 znaků pro eliptický křivku a pro podporované skupiny.

Standardní specifikace je `00210023002400250019`. Je-li povolen protokol TLS V1.3 , je k konec výchozího seznamu připojen řetězec `0029 (x25519)` .

Identifikace a ověřování uživatelů

Uživatele můžete identifikovat a ověřovat pomocí certifikátů X.509 , struktury MQCSP nebo několika typů uživatelského ukončovacího programu.

Použití certifikátů X.509

Uživatele můžete identifikovat a ověřovat pomocí certifikátů x.509 s parametrem **CHLAUTH** a argumentem **SSLPEER** . Parametr **SSLPEER** určuje filtr, který má být použit k porovnání s rozlišujícím názvem subjektu certifikátu od správce front typu peer nebo od klienta na druhém konci kanálu.

Další informace o použití příkazu **CHLAUTH** a parametru **SSLPEER** naleznete v části SET CHLAUTH.

Použití struktury MQCSP

Strukturu parametrů zabezpečení připojení MQCSP lze zadat ve volání MQCONNX; tato struktura obsahuje ID uživatele a heslo. Je-li to nutné, můžete změnit MQCSP v uživatelské proceduře zabezpečení.

Poznámka: Správce oprávnění k objektu (OAM) nepoužívá heslo. Avšak OAM má určitou omezenou práci s ID uživatele, které lze považovat za triviální formu ověření. Tyto kontroly přestanou přijímat další ID uživatele, používáte-li tyto parametry ve svých aplikacích.

Varování: V některých případech se heslo ve struktuře MQCSP pro klientskou aplikaci odešle přes síť jako prostý text. Chcete-li zajistit, aby hesla klienta aplikace byla chráněna správně, prohlédněte si téma “Ochrana heslem MQCSP” na stránce 29.

Implementace identifikace a ověření v uživatelských procedurách zabezpečení

Primárním účelem uživatelské procedury zabezpečení je umožnit agentovi MCA na každém konci kanálu ověřovat jeho partnera. Na každém konci kanálu zpráv a na konci kanálu kanálu MQI agent MCA obvykle jedná jménem správce front, ke kterému je připojen. Na konci klienta kanálu MQI se agent MCA obvykle chová jménem uživatele klientské aplikace produktu IBM MQ . V této situaci probíhá vzájemná ověření mezi dvěma správci front nebo mezi správcem front a uživatelem aplikace produktu IBM MQ MQI client .

Dodaná uživatelská procedura zabezpečení (uživatelská procedura kanálu SSPI) ilustruje, jak lze vzájemné ověření implementovat pomocí výměny tokenů ověření, které jsou generovány, a poté zkontrolovány důvěryhodným ověřovacím serverem, jako je například Kerberos. Další informace naleznete v tématu “Ukončovací program kanálu SSPI v systému Windows” na stránce 149.

Vzájemné ověření lze také implementovat pomocí technologie PKI (Public Key Infrastructure (PKI)). Každá uživatelská procedura zabezpečení generuje některá náhodná data a podepisuje ji pomocí soukromého klíče správce front nebo uživatele, který reprezentuje, a odešle podepsaná data partnerovi ve zprávě zabezpečení. Uživatelská procedura zabezpečení ochrany dat provádí ověření pomocí kontroly digitálního podpisu pomocí veřejného klíče správce front nebo uživatele. Před výměnou digitálních podpisů může být nutné, aby při generování kódu digest zprávy došlo k souhlasu s algoritmem zabezpečení, pokud je pro použití k dispozici více než jeden algoritmus.

Pokud uživatelská procedura zabezpečení odešle podepsaná data svému partnerovi, musí také odeslat nějaké prostředky identifikující správce front nebo uživatele, kterého zastupuje. Může se jednat o rozlišující název, nebo dokonce o digitální certifikát. Je-li odeslán digitální certifikát, může uživatelská procedura zabezpečení partnera ověřit certifikát tak, že bude pracovat prostřednictvím řetězce certifikátů do kořenového certifikátu CA. Tím se poskytuje ujištění o vlastnictví veřejného klíče, který se používá ke kontrole digitálního podpisu.

Partner pro zabezpečení ochrany dat může ověřit digitální certifikát pouze v případě, že má přístup k úložišti klíčů, které obsahuje zbývající certifikáty v řetězu certifikátů. Pokud není odeslán digitální certifikát pro správce front nebo uživatele, musí být k dispozici v úložišti klíčů, ke kterému má přístup partnerská uživatelská procedura přístup. Uživatelská procedura zabezpečení partnera nemůže zkontrolovat digitální podpis, pokud nemůže najít veřejný klíč podepisujícího subjektu.

Transport Layer Security (TLS) používá techniky PKI jako ty, které právě popisují. Další informace o tom, jak TLS provádí ověření, viz “Koncepce zabezpečení přenosové vrstvy (TLS)” na stránce 14.

Není-li k dispozici důvěryhodný ověřovací server nebo podpora PKI, mohou být použity jiné techniky. Běžnou techniku, kterou lze implementovat do uživatelských procedur zabezpečení, je použít algoritmus symetrického klíče.

Jedna z uživatelských procedur zabezpečení, ukončení A, vygeneruje náhodné číslo a odešle ji ve zprávě o zabezpečení do své uživatelské procedury zabezpečení partnerského serveru, ukončete program B. Exit B šifruje číslo pomocí její kopie klíče, která je známa pouze dvěma uživatelským procedurám zabezpečení. Uživatelská procedura B odešle šifrované číslo ukončení A ve zprávě zabezpečení s druhým náhodným číslem, které výstupní bod B vygeneroval. Exit A ověří, že první náhodné číslo bylo zašifrováno správně, zašifruje druhé náhodné číslo pomocí její kopie klíče a odešle zašifrované číslo, aby se zakódované B ve

zprávě zabezpečení. Ukončete B, pak ověříte, že druhé náhodné číslo bylo správně zašifrováno. Pokud při této výměně není ukončena žádná uživatelská procedura zabezpečení s autenticitou jiného, může program MCA předat pokyn k uzavření kanálu.

Výhodou této techniky je, že během výměny nedochází k odeslání klíče nebo hesla přes komunikační spojení. Nevýhodou je, že neposkytuje řešení problému, jak zajistit distribuci sdíleného klíče bezpečným způsobem. Jeden z řešení tohoto problému je popsán v tématu “Implementace utajení v uživatelských ukončovacích programech” na stránce 456. Podobná technika se používá v SNA pro vzájemné ověření dvou jednotek LU při vytváření vazby k vytvoření relace. Technika je popsána v tématu “Ověření úrovně relace” na stránce 115.

Všechny předchozí techniky pro vzájemné ověření mohou být přizpůsobeny tak, aby poskytovaly jednosměrné ověření.

Implementace identifikace a ověření ve výstupních procedurách zprávy

Když aplikace vloží zprávu do fronty, pole *UserIdentifier* v deskriptoru zprávy obsahuje ID uživatele přidružené k aplikaci. Avšak nejsou přítomna žádná data, která by mohla být použita k ověření ID uživatele. Tato data mohou být přidána uživatelskou procedurou pro odeslání zprávy na odesílající straně kanálu a kontrolována ukončením zprávy na přijímajícím konci kanálu. Ověřující data mohou být šifrovaným heslem nebo digitálním podpisem, například.

Tato služba může být efektivnější, pokud je implementována na úrovni aplikace. Základním požadavkem je pro uživatele aplikace, která přijímá zprávu, aby bylo možné identifikovat a ověřit uživatele aplikace, která odeslala zprávu. Je proto přirozené zvážit zavedení této služby na úrovni aplikace. Další informace viz “Mapování identity ve výstupu rozhraní API a ukončení přeletu rozhraní API” na stránce 329.

Implementace identifikace a ověření ve výstupu rozhraní API a ukončení přeletu rozhraní API

Na úrovni jednotlivé zprávy, identifikace a ověření je služba, která zahrnuje dva uživatele, odesílatele a příjemce zprávy. Základním požadavkem je pro uživatele aplikace, která přijímá zprávu, aby bylo možné identifikovat a ověřit uživatele aplikace, která odeslala zprávu. Všimněte si, že požadavek je jednosměrný, nikoli dvoucestný, ověření.

V závislosti na tom, jak je implementováno, mohou uživatelé a jejich aplikace potřebovat rozhraní nebo dokonce interakci s danou službou. Kromě toho, kdy a jak může být služba použita, může záviset na tom, kde jsou uživatelé a jejich aplikace vyhledány, a na povaze samotných aplikací. Je proto přirozené uvažovat o implementaci služby spíše na úrovni aplikace než na úrovni odkazů.

Pokud uvažujete o implementaci této služby na úrovni propojení, budete možná muset řešit problémy jako jsou následující:

- Na kanálu zpráv jak použijete službu pouze na ty zprávy, které to vyžadují?
- Jak můžete povolit uživatelům a jejich aplikacím rozhraní nebo interakci s touto službou, pokud se jedná o požadavek?
- Ve víceuzlové situaci, kdy je zpráva odeslána přes více než jeden kanál zpráv na cestě do místa určení, kde vyvoláte komponenty služby?

Zde je uvedeno několik příkladů, jak lze službu identifikace a ověření implementovat na úrovni aplikace. Termín *ukončení rozhraní API* znamená buď uživatelskou proceduru rozhraní API, nebo uživatelskou proceduru pro překročení rozhraní API.

- Když aplikace vloží zprávu do fronty, může uživatelská procedura rozhraní API získat token ověření z důvěryhodného ověřovacího serveru, jako je například Kerberos. Uživatelská procedura rozhraní API může přidat tento token do dat aplikace ve zprávě. Při načtení zprávy přijímající aplikací může druhá uživatelská procedura rozhraní API požádat ověřovací server, aby ověřil odesílatele, a to tak, že zkontroluje token.
- Když aplikace vloží zprávu do fronty, může uživatelská procedura rozhraní API připojit k datům aplikace ve zprávě následující položky:

- Digitální certifikát odesílatele
- Digitální podpis odesílatele

Pokud jsou k dispozici různé algoritmy pro generování kódu digest zprávy, může uživatelská procedura rozhraní API zahrnovat název algoritmu, který používá.

Když je zpráva načtena přijímající aplikací, může druhá uživatelská procedura rozhraní API provádět následující kontroly:

- Uživatelská procedura rozhraní API může ověřit digitální certifikát tak, že bude pracovat prostřednictvím řetězce certifikátů do kořenového certifikátu CA. K tomu musí mít uživatelská procedura rozhraní API přístup ke klíčovému úložišti, které obsahuje zbývající certifikáty v řetězu certifikátů. Tato kontrola zabezpečuje ujištění, že odesilatel, identifikovaný rozlišujícím názvem, je skutečným vlastníkem veřejného klíče obsaženého v certifikátu.
- Uživatelská procedura rozhraní API může kontrolovat digitální podpis pomocí veřejného klíče obsaženého v certifikátu. Tato kontrola ověřuje odesílatele.

Rozlišovací jméno odesilatele může být odesláno místo celého digitálního certifikátu. V takovém případě musí úložiště klíčů obsahovat certifikát odesílatele, aby druhá uživatelská procedura rozhraní API mohla najít veřejný klíč odesilatele. 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, může uživatelská procedura rozhraní API připojit některá data, jako je například zašifrované heslo, k datům aplikace ve zprávě. Když je zpráva načtena přijímající aplikací, druhá uživatelská procedura rozhraní API může ověřit ID uživatele pomocí dat, která se urazila se zprávou.

  Tato technika může být považována za dostatečnou pro zprávy, které pocházejí z řízeného a důvěryhodného prostředí, a za okolností, kdy není k dispozici důvěryhodný ověřovací server nebo podpora PKI.

PAM (Pluggable Authentication Method)

Linux AIX

Modul PAM je nyní běžný na všech platformách UNIX and Linux a poskytuje obecný mechanizmus, který skrývá podrobnosti o ověření uživatele ze služeb.

Pro různé služby lze použít různá pravidla ověření, a to konfigurací pravidel, bez nutnosti změn pro samotné služby.

Další informace viz “Použití metody PAM (Pluggable Authentication Method)” na stránce 341.

Oprávnění uživatelé

Privilegovaný uživatel je takový, který má úplná administrativní oprávnění pro produkt IBM MQ.

Kromě uživatelů uvedených v následující tabulce jsou k dispozici určité objekty a autorizace, pro které je třeba při udílení přístupu zajistit zvýšenou péči, aby byla zajištěna integrita a zabezpečení správce front. Přebytečná kontrola se musí uplatnit při udělení některé z těchto povolení:

- Libovolná oprávnění k objektům produktu SYSTEM
- Oprávnění administrace pro vytváření, změny a odstraňování objektů.

  z/OS V systému z/OSje toto oprávnění oprávněním k zabezpečení příkazů a oprávnění k zabezpečení prostředků pro vydávání příkazů DEFINE, ALTER a DELETE.

  Multi Na všech ostatních platformách jsou tato oprávnění administračními autorizacemi, jako jsou `+crt`, `+chg` a `+dlt`.
- Autorizace administrace pro vymazání front.

z/OS V systému z/OSje toto oprávnění oprávněním k zabezpečení příkazů a oprávnění zabezpečení prostředků příkazů k vydávání příkazů CLEAR.

Multi Na všech ostatních platformách toto oprávnění je `+clr`.

- Autorizace administrace pro zastavení kanálů, odvolání nebo potvrzení zpráv.

  z/OS V systému z/OSje toto oprávnění oprávněním zabezpečení příkazů a oprávnění zabezpečení prostředků příkazů k vydání příkazů, jako je RESET CHANNEL, START CHANNEL a STOP CHANNEL.

  Multi Na všech ostatních platformách jsou tato oprávnění `+ctrl` a `+ctrlx`.
- Alternativní autorizace uživatele MQI, která umožňuje aplikacím eskalovat oprávnění pro kontroly autorizace.

  z/OS V systému z/OSje toto oprávnění uděleno každému oprávnění uděleného pro profily zabezpečení alternativního uživatele.

  Multi Na všech ostatních platformách toto oprávnění je `+altusr`.
- Kontextové autorizace, které umožňují aplikacím měnit kontext zabezpečení zpráv.

  z/OS V systému z/OSje toto oprávnění uděleno každému oprávnění uděleného profilům zabezpečení kontextu.

  Multi Na všech ostatních platformách jsou tato oprávnění `+setall` a `+setid`.

Aplikace systému zpráv by jako obecné činitele měly mít pouze základní autorizace MQI pro fronty nebo témata, které jsou potřebné. Kanály MCA, které jsou spouštěny v rámci neprivilegovaného objektu MCAUSER a některých dalších speciálních typů aplikací, jako jsou například obslužné rutiny front nedoručených zpráv, mohou vyžadovat další autorizace, které nejsou normálně poskytovány aplikacím, aby fungovaly správně.

Tabulka 67. Oprávnění uživatelé podle platformy

Platforma	**Oprávnění uživatelé**
Systémy Windows	• SYSTÉM • Členové skupiny mqm • Členové skupiny administrátorů
Systémy AIX and Linux	• Členové skupiny mqm
IBM i IBM i Systémy IBM i	• Profily qmqm a qmqmadm • Všechny členy skupiny qmqmadm • Jakýkoli uživatel definovaný s nastavením *ALLOBJ
z/OS	ID uživatele, pod kterým jsou spuštění adresní prostory pro iniciátor kanálu, správce front a rozšířené zabezpečení zpráv. Tato ID uživatele nemají automaticky úplná administrativní oprávnění pro IBM MQ, ale jsou považována za privilegovanou vzhledem k úrovni přístupu, která je obvykle udělena těmto ID uživatelů.

Identifikace a ověřování uživatelů pomocí struktury MQCSP

Můžete určit strukturu parametrů zabezpečení připojení MQCSP ve volání MQCONNX.

Struktura parametrů zabezpečení připojení MQCSP obsahuje ID uživatele a heslo, které může autorizační služba použít k identifikaci a ověření uživatele.

Můžete změnit MQCSP v uživatelské proceduře zabezpečení.

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 aplikace klienta odpovídajícím způsobem chráněna, prohlédněte si téma "Ochrana heslem MQCSP" na stránce 29.

Relace mezi nastaveními MQCSP a AdoptCTX

Produkt IBM MQ vždy ověřuje pověření předaná prostřednictvím struktury MQCSP, pokud není povolena funkce ověřování připojení. Jakmile jsou pověření úspěšně ověřena, produkt IBM MQ se pokusí převzít ID uživatele pro budoucí kontroly autorizace, pokud není volba nedostane povolení.

Produkt IBM MQ má limit délky ID uživatelů, které může použít pro kontroly autorizace. Tyto limity jsou podrobně popsány v části "ID uživatelů" na stránce 82. Při adoptování ID uživatele předaného prostřednictvím struktury MQCSP se IBM MQ chová odlišně v závislosti na dalších volbách konfigurace:

- Při použití ověření připojení LDAP produkt IBM MQ načte hodnotu pole nastavenou v parametru SHORTUSR ze záznamu uživatele LDAP daného uživatele a převezme toto ID uživatele.

  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 obj.CTX YES, je ID uživatele předané prostřednictvím struktury 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 u konfigurace CONNAUTH AUTHINFO volbu SERVIS (NO) a alternativní přístup, jako např. pravidlo CHLAUTH USERMAP, uživatelská procedura zabezpečení nebo nastavení objektu kanálu MCAUSER, abyste nastavili ID uživatele pro kanál.

Implementace identifikace a ověření v uživatelských procedurách zabezpečení

Ukončení zabezpečení můžete použít k implementaci jednosměrného nebo vzájemného ověření.

Primárním účelem uživatelské procedury zabezpečení je umožnit agentovi MCA na každém konci kanálu ověřovat jeho partnera. Na každém konci kanálu zpráv a na konci kanálu kanálu MQI agent MCA obvykle jedná jménem správce front, ke kterému je připojen. Na konci klienta kanálu MQI se agent MCA obvykle chová jménem uživatele aplikace IBM MQ MQI client . V této situaci probíhá vzájemná ověření mezi dvěma správci front nebo mezi správcem front a uživatelem aplikace produktu IBM MQ MQI client .

Dodaná uživatelská procedura zabezpečení (uživatelská procedura kanálu SSPI) ilustruje, jak lze vzájemné ověření implementovat pomocí výměny tokenů ověření, které jsou generovány, a poté

zkontrolovány důvěryhodným ověřovacím serverem, jako je například Kerberos. Další informace naleznete v tématu "Ukončovací program kanálu SSPI v systému Windows" na stránce 149.

Vzájemné ověření lze také implementovat pomocí technologie PKI (Public Key Infrastructure (PKI)). Každá uživatelská procedura zabezpečení generuje některá náhodná data a podepisuje ji pomocí soukromého klíče správce front nebo uživatele, který reprezentuje, a odešle podepsaná data partnerovi ve zprávě zabezpečení. Uživatelská procedura zabezpečení ochrany dat provádí ověření pomocí kontroly digitálního podpisu pomocí veřejného klíče správce front nebo uživatele. Před výměnou digitálních podpisů může být nutné, aby při generování kódu digest zprávy došlo k souhlasu s algoritmem zabezpečení, pokud je pro použití k dispozici více než jeden algoritmus.

Pokud uživatelská procedura zabezpečení odešle podepsaná data svému partnerovi, musí také odeslat nějaké prostředky identifikující správce front nebo uživatele, kterého zastupuje. Může se jednat o rozlišující název, nebo dokonce o digitální certifikát. Je-li odeslán digitální certifikát, může uživatelská procedura zabezpečení partnera ověřit certifikát tak, že bude pracovat prostřednictvím řetězce certifikátů do kořenového certifikátu CA. Tím se poskytuje ujištění o vlastnictví veřejného klíče, který se používá ke kontrole digitálního podpisu.

Partner pro zabezpečení ochrany dat může ověřit digitální certifikát pouze v případě, že má přístup k úložišti klíčů, které obsahuje zbývající certifikáty v řetězu certifikátů. Pokud není odeslán digitální certifikát pro správce front nebo uživatele, musí být k dispozici v úložišti klíčů, ke kterému má přístup partnerská uživatelská procedura přístup. Uživatelská procedura zabezpečení partnera nemůže zkontrolovat digitální podpis, pokud nemůže najít veřejný klíč podepisujícího subjektu.

Transport Layer Security (TLS) používá techniky PKI jako ty, které právě popisují. Další informace o tom, jak zabezpečení SSL provádí ověřování, najdete v tématu "Koncepce zabezpečení přenosové vrstvy (TLS)" na stránce 14.

Není-li k dispozici důvěryhodný ověřovací server nebo podpora PKI, mohou být použity jiné techniky. Běžnou techniku, kterou lze implementovat do uživatelských procedur zabezpečení, je použít algoritmus symetrického klíče.

Jedna z uživatelských procedur zabezpečení, ukončení A, vygeneruje náhodné číslo a odešle ji ve zprávě o zabezpečení do své uživatelské procedury zabezpečení partnerského serveru, ukončete program B. Exit B šifruje číslo pomocí její kopie klíče, která je známa pouze dvěma uživatelským procedurám zabezpečení. Uživatelská procedura B odešle šifrované číslo ukončení A ve zprávě zabezpečení s druhým náhodným číslem, které výstupní bod B vygeneroval. Exit A ověří, že první náhodné číslo bylo zašifrováno správně, zašifruje druhé náhodné číslo pomocí její kopie klíče a odešle zašifrované číslo, aby se zakódované B ve zprávě zabezpečení. Ukončete B, pak ověříte, že druhé náhodné číslo bylo správně zašifrováno. Pokud při této výměně není ukončena žádná uživatelská procedura zabezpečení s autenticitou jiného, může program MCA předat pokyn k uzavření kanálu.

Výhodou této techniky je, že během výměny nedochází k odeslání klíče nebo hesla přes komunikační spojení. Nevýhodou je, že neposkytuje řešení problému, jak zajistit distribuci sdíleného klíče bezpečným způsobem. Jeden z řešení tohoto problému je popsán v tématu "Implementace utajení v uživatelských ukončovacích programech" na stránce 456. Podobná technika se používá v SNA pro vzájemné ověření dvou jednotek LU při vytváření vazby k vytvoření relace. Technika je popsána v tématu "Ověření úrovně relace" na stránce 115.

Všechny předchozí techniky pro vzájemné ověření mohou být přizpůsobeny tak, aby poskytovaly jednosměrné ověření.

Mapování identit ve výstupních procedurách zprávy

Můžete použít uživatelské procedury pro zpracování informací k ověření totožnosti uživatele, ačkoli by mohlo být lepší implementovat ověření na úrovni aplikace.

Když aplikace vloží zprávu do fronty, pole *UserIdentifier* v deskriptoru zprávy obsahuje ID uživatele přidružené k aplikaci. Avšak nejsou přítomna žádná data, která by mohla být použita k ověření ID uživatele. Tato data mohou být přidána uživatelskou procedurou pro odeslání zprávy na odesílající straně kanálu a kontrolována ukončením zprávy na přijímajícím konci kanálu. Ověřující data mohou být šifrovaným heslem nebo digitálním podpisem, například.

Tato služba může být efektivnější, pokud je implementována na úrovni aplikace. Základním požadavkem je pro uživatele aplikace, která přijímá zprávu, aby bylo možné identifikovat a ověřit uživatele aplikace, která odeslala zprávu. Je proto přirozené zvážit zavedení této služby na úrovni aplikace. Další informace viz "Mapování identity ve výstupu rozhraní API a ukončení přeletu rozhraní API" na stránce 329.

Mapování identity ve výstupu rozhraní API a ukončení přeletu rozhraní API

Aplikace, která přijme zprávu, musí být schopna identifikovat a ověřit uživatele aplikace, která odeslala zprávu. Tato služba je obvykle nejlépe implementována na úrovni aplikace. Uživatelské procedury rozhraní API mohou službu implementovat v mnoha ohledech.

Na úrovni jednotlivé zprávy, identifikace a ověření je služba, která zahrnuje dva uživatele, odesílatele a příjemce zprávy. Základním požadavkem je pro uživatele aplikace, která přijímá zprávu, aby bylo možné identifikovat a ověřit uživatele aplikace, která odeslala zprávu. Všimněte si, že požadavek je jednosměrný, nikoli dvoucestný, ověření.

V závislosti na tom, jak je implementováno, mohou uživatelé a jejich aplikace potřebovat rozhraní nebo dokonce interakci s danou službou. Kromě toho, kdy a jak může být služba použita, může záviset na tom, kde jsou uživatelé a jejich aplikace vyhledány, a na povaze samotných aplikací. Je proto přirozené uvažovat o implementaci služby spíše na úrovni aplikace než na úrovni odkazů.

Pokud uvažujete o implementaci této služby na úrovni propojení, budete možná muset řešit problémy jako jsou následující:

- Na kanálu zpráv jak použijete službu pouze na ty zprávy, které to vyžadují?
- Jak můžete povolit uživatelům a jejich aplikacím rozhraní nebo interakci s touto službou, pokud se jedná o požadavek?
- Ve víceuzlové situaci, kdy je zpráva odeslána přes více než jeden kanál zpráv na cestě do místa určení, kde vyvoláte komponenty služby?

Zde je uvedeno několik příkladů, jak lze službu identifikace a ověření implementovat na úrovni aplikace. Termín *ukončení rozhraní API* znamená buď uživatelskou proceduru rozhraní API, nebo uživatelskou proceduru pro překročení rozhraní API.

- Když aplikace vloží zprávu do fronty, může uživatelská procedura rozhraní API získat token ověření z důvěryhodného ověřovacího serveru, jako je například Kerberos. Uživatelská procedura rozhraní API může přidat tento token do dat aplikace ve zprávě. Při načtení zprávy přijímající aplikací může druhá uživatelská procedura rozhraní API požádat ověřovací server, aby ověřil odesílatele, a to tak, že zkontroluje token.
- Když aplikace vloží zprávu do fronty, může uživatelská procedura rozhraní API připojit k datům aplikace ve zprávě následující položky:
  - Digitální certifikát odesílatele
  - Digitální podpis odesílatele

  Pokud jsou k dispozici různé algoritmy pro generování kódu digest zprávy, může uživatelská procedura rozhraní API zahrnovat název algoritmu, který používá.

  Když je zpráva načtena přijímající aplikací, může druhá uživatelská procedura rozhraní API provádět následující kontroly:

  - Uživatelská procedura rozhraní API může ověřit digitální certifikát tak, že bude pracovat prostřednictvím řetězce certifikátů do kořenového certifikátu CA. K tomu musí mít uživatelská procedura rozhraní API přístup ke klíčovému úložišti, které obsahuje zbývající certifikáty v řetězu certifikátů. Tato kontrola zabezpečuje ujištění, že odesilatel, identifikovaný rozlišujícím názvem, je skutečným vlastníkem veřejného klíče obsaženého v certifikátu.
  - Uživatelská procedura rozhraní API může kontrolovat digitální podpis pomocí veřejného klíče obsaženého v certifikátu. Tato kontrola ověřuje odesílatele.

  Rozlišovací jméno odesilatele může být odesláno místo celého digitálního certifikátu. V takovém případě musí úložiště klíčů obsahovat certifikát odesílatele, aby druhá uživatelská procedura rozhraní API mohla najít veřejný klíč odesilatele. 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, může uživatelská procedura rozhraní API připojit některá data, jako je například zašifrované heslo, k datům aplikace ve zprávě. Když je zpráva načtena přijímající aplikací, druhá uživatelská procedura rozhraní API může ověřit ID uživatele pomocí dat, která se urazila se zprávou.

  Tato technika může být považována za dostatečnou pro zprávy, které pocházejí z řízeného a důvěryhodného prostředí, a za okolností, kdy není k dispozici důvěryhodný ověřovací server nebo podpora PKI.

Práce se zrušenými certifikáty

Digitální certifikáty mohou být odvolány vydavateli certifikátů. Stav odvolání certifikátů můžete zkontrolovat pomocí protokolu OCSP nebo seznamů odvolaných certifikátů na serverech LDAP v závislosti na platformě.

Během komunikace výměnou potvrzení TLS se vzájemně komunikují s digitálními certifikáty. Ověření může zahrnovat i kontrolu, zda je přijatý certifikát nadále důvěryhodný. Vydavatelé certifikátů (CA) odvolají certifikáty z různých důvodů, včetně:

- Vlastník byl přesunut do jiné organizace
- Soukromý klíč již není tajný.

CA publikují odvolané osobní certifikáty v seznamu odvolaných certifikátů (CRL). Certifikáty CA, které byly zrušeny, jsou publikovány v ARL (Authority Revocation List).

ALW Na platformách AIX, Linux, and Windows podpora zabezpečení SSL produktu IBM MQ zjišťuje 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 zabezpečení SSL produktu IBM MQ kontroluje odvolané certifikáty pomocí seznamů CRL a ARL pouze na serverech LDAP.

Další informace o certifikačních autorech najdete v tématu “digitální certifikáty” na stránce 9.

Kontrola OCSP/CRL

Kontrola protokolu OCSP (Online Certificate Status Protocol) /CRL (Certificate Revocation List) se provádí proti vzdáleným příchozím certifikátům. Proces zkontroluje celý řetězec, který se podílí na osobním certifikátu vzdáleného systému, až po jeho kořenový certifikát.

Ověření protokolu OCSP pomocí příkazu openSSL

Pokud váš podnik používá openSSL k ověření protokolu OCSP a pak se pokusíte použít připojení GSKit TLS, obdržíte varovnou zprávu o stavu NEZNÁMÝ.

Důvodem je to, že všechny certifikáty v řetězci, kromě kořene, jsou zkontrolovány sadou GSKit pro stav odvolání. Operace GSKit je v souladu s RFC 5280 a je to popsáno v zásadě důvěryhodnosti GSKit. Algoritmus GSKit se pokusí o všechny dostupné zdroje informací o odvolání, jak je popsáno v RFC 5280 a v zásadě důvěryhodnosti GSKit.

Jak pracuje kontrola OCSP/CRL v produktu IBM MQ?

Produkt IBM MQ podporuje dva mechanizmy pro řízení chování při kontrole certifikátů proti pojmenovaným koncovým bodům OCSP nebo CRL, a to buď v rozšíření certifikátu, nebo v případě, že jsou definovány v objektech AUTHINFO:

- Atributy **OCSPCheckExtensions**, **CDPCheckExtensions**a **OCSPAuthentication** ze sekce SSL souboru qm.inia
- Použití parametru SSLCRLNL správce front a konfigurací OCSP a CRLLDAP protokolu AUTHINFO. Další informace viz ALTER AUTHINFO a ALTER QMGR .

Upozornění:

Příkaz ALTER AUTHINFO s produktem **AUTHTYPE(OCSP)** se nepoužívá pro použití ve správcích front IBM i nebo z/OS . Lze však zadat na těchto platformách, aby se zkopírovaly do tabulky definic kanálů klienta (CCDT) pro klientské použití.

Atributy stano **OCSPCheckExtensions** a **CDPCheckExtensions** SSL řídí, zda produkt IBM MQ ověří certifikát proti protokolu OCSP nebo serveru CRL, který je podrobně popsán v rozšíření certifikátu AIA certifikátu.

Není-li tato možnost povolena, protokol OCSP nebo CRL v rozšíření certifikátu se nekontaktuje.

Pokud jsou protokoly OCSP nebo CRL podrobně popsány pomocí objektů AUTHINFO a odkazovány pomocí atributu SSLCRLNL **QMGR** , pak během zpracování odvolání certifikátů se produkt IBM MQ pokusí kontaktovat tyto servery.

Důležité: V seznamu názvů SSLCRLNL může být definován pouze jeden objekt OCSP AUTHINFO.

Pokud:

OCSPCheckExtensions= NO a **CDPCheckExtensions**=*NO* jsou nastaveny a
V objektech AUTHINFO nejsou definovány žádné servery OCSP nebo CRL

neprovádí se žádná kontrola odvolání certifikátu.

Při ověřování certifikátu pro jeho stav odvolání produkt IBM MQ kontaktuje protokol OCSP nebo seznam serverů CRL uvedený v následujícím pořadí, pokud je povolen:

1. Server OCSP je podrobně popsán v objektu **AUTHTYPE(OCSP)** a odkazuje se na něj v atributu SSLCRLNL **QMGR** .
2. Servery OCSP podrobně uvedené v rozšíření AIA certifikátů, pokud je **OCSPCheckExtensions**=*YES*.
3. Servery CRL jsou podrobně popsány v rozšíření **CRLDistributionPoints** certifikátů, pokud je **CDPCheckExtensions** =*YES*.
4. Všechny servery CRL, které jsou podrobně popsány v objektech **AUTHINFO(CRLLDAP)** a jsou odkazovány v atributu SSLCRLNL **QMGR** .

Při ověřování certifikátu se v případě, že krok na serveru OCSP nebo na serveru CRL vrátí definitivní odpověď REVOKED nebo VALID na dotaz na certifikát, neprovedou se žádné další kontroly a stav certifikátu, jak je prezentován, se používá 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 jsou vyčerpány všechny možnosti.

Chování, zda je certifikát považován za zrušený, nelze-li jeho stav určit, se liší pro OCSP a servery CRL:

- Pro servery CRL, pokud nelze získat seznam CRL, je certifikát považován za NOT_REVOKED
- Pokud v případě serverů OCSP nelze získat stav odvolání z pojmenovaného serveru OCSP, bude chování řízeno atributem **OCSPAuthentication** v sekci SSL Stanza souboru qm.ini .

  Tento atribut můžete nakonfigurovat tak, aby blokoval připojení, povolit připojení nebo povolit připojení s varovnou zprávou.

Podle potřeby můžete použít atribut **SSLHTTPProxyName**=*string* ve stanze SSL souboru qm.ini a mqclient.ini pro kontroly OCSP. Řetězec je buď název hostitele, nebo síťová adresa serveru proxy HTTP, který má sada GSKit použít pro kontroly OCSP.

V IBM MQ 9.1.5 můžete nastavit hodnotu **OCSPTimeout** ve stanze SSL u souborů `qm.ini` nebo `mqclient.ini` , které nastaví počet sekund, po které se má čekat 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 IBM MQ v systémech AIX, Linux, and Windows .

Chcete-li zkontrolovat stav odvolání digitálního certifikátu pomocí protokolu OCSP, produkt IBM MQ může použít dvě metody k určení odpovídacího modulu OCSP, který má být kontaktován:

- 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 udržován v jednom z následujících umístění:

- Linux AIX V oddílu SSL souboru `qm.ini` v systému AIX and Linux.
- Windows V registru Windows .

Tento atribut lze nastavit pomocí IBM MQ Explorer. U klientů se atribut nachází 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 žádné další certifikáty. Kroky, které jste již přijali pro vytvoření konektivity 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. Protože je odezva OCSP odeslána s certifikátem, který ji podepsal (a tento certifikát je podepsán CA, který je již důvěryhodný pro připojení TLS), není třeba 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. Kopii certifikátu odpovídacího modulu OCSP je nutné přidat do databáze klíčů klienta nebo správce front, který provádí kontrolu OCSP. Viz “Přidání certifikátu CA nebo veřejné části certifikátu podepsaného (svým držitelem) do úložiště klíčů v systému AIX, Linux, and Windows” na stránce 297. 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 odezvě OCSP a kontrola protokolu OCSP má za následek Neznámý výsledek, který může způsobit zavření kanálu produktem IBM MQ v závislosti na hodnotě prvku OCSPAuthentication.

Protokol OCSP (Online Certificate Status Protocol) v aplikacích klienta Java a JMS

Kvůli omezení rozhraní API produktu Java může produkt IBM MQ použít kontrolu odvolání certifikátů protokolu OCSP (Online Certificate Status Protocol) pro zabezpečené sokety TLS pouze v případě, že je protokol OCSP povolen pro celý proces virtuálního počítače (JVM) produktu Java . 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 soubor java.security.Security.setProperty() Rozhraní API, v závislosti na platné zásadě produktu 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`.

Název vlastnosti	Popis
	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 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 by tato konfigurace mohla mít nežádoucí vedlejší účinky, je-li 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. Dávejte pozor, když použijete prozatímní opravy produktu Java a údržbu produktu, abyste se vyhnuli 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 komponentu AMS Java Interceptor popsanou v tématu Povolení kontroly OCSP v nativních zachytávačích, dbejte na to, abyste se vyhnuli použití konfigurace protokolu OCSP java.security , která je v konfliktu s konfigurací AMS OCSP v konfiguračním souboru úložiště klíčů.

Práce se seznamy odvolaných certifikátů a seznamy odvolaných autorit

Podpora IBM MQ pro seznamy CRL a ARL se liší podle platformy.

Podpora CRL a ARL na každé platformě je následující:

- V systému z/OSSystem SSL podporuje seznamy CRL a ARL uložené na serverech LDAP produktem Tivoli Public Key Infrastructure.
- Na jiných platformách podpora CRL a ARL odpovídá doporučením profilu PKIX X.509 V2 profilu CRL.

Produkt IBM MQ udržuje mezipaměť seznamů CRL a ARL, k nimž bylo přistupována během předchozích 12 hodin.

Když správce front nebo IBM MQ MQI client obdrží certifikát, zkontroluje seznam CRL a potvrdí, že je certifikát stále platný. IBM MQ první kontroly v mezipaměti, pokud existuje mezipaměť. Pokud seznam CRL není uložen v mezipaměti, produkt IBM MQ dotazuje umístění serveru LDAP CRL v pořadí, v jakém se vyskytují v seznamu názvů objektů ověřovacích informací určených atributem *SSLCRLNL* , dokud produkt IBM MQ nenajde dostupný seznam CRL. Není-li seznam názvů zadán nebo je-li zadán s prázdnou hodnotou, seznamy odvolaných certifikátů se nekontrolují.

Nastavení serverů LDAP

Konfigurujte strukturu stromu informací adresáře LDAP tak, aby odrážela hierarchii rozlišujících názvů certifikačních autorit. To lze provést pomocí souborů formátu výměny dat LDAP.

Konfigurujte strukturu DIT (Directory Information Tree) LDAP pro použití hierarchie odpovídající rozlišujícím názvům certifikačních úřadů, které vydávají certifikáty a seznamy CRL. Strukturu DIT můžete nastavit pomocí souboru, který používá formát LDIF (LDAP Data Interchange Format). K aktualizaci adresáře můžete také použít soubory LDIF.

Soubory LDIF jsou textové soubory ASCII, které obsahují informace požadované pro definování objektů v rámci adresáře LDAP. Soubory LDIF obsahují jednu nebo více záznamů, z nichž každá obsahuje rozlišující název, alespoň jednu definici třídy objektu a volitelně více definic atributu.

Atribut `certificateRevocationList;binary` obsahuje v binární formě seznam odvolaných uživatelských certifikátů. Atribut `authorityRevocationList;binary` obsahuje binární seznam certifikátů CA, které byly odvolány. Pro použití s produktem IBM MQ TLS musí binární data pro tyto atributy odpovídat formátu DER (Definite Encoding Rules). Další informace o souborech LDIF najdete v dokumentaci dodávané se serverem LDAP.

Obrázek 20 na stránce 336 ukazuje vzorový soubor LDIF, který můžete vytvořit jako vstup na server LDAP pro načtení seznamů CRL a ARL vydaných CA1, což je fiktivní vydavatel certifikátů s rozlišujícím názvem "CN=CA1, OU=Test, O=IBM, C=GB", který je nastaven organizací Test v rámci produktu IBM.

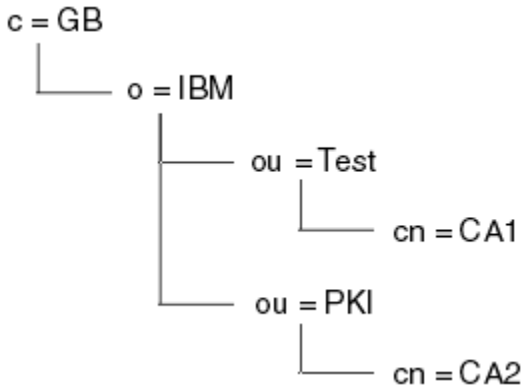
```
dn: o=IBM, c=GB
o: IBM
objectclass: top
objectclass: organization

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 336 ukazuje strukturu DIT, kterou váš server LDAP vytváří při načtení ukázkového souboru LDIF zobrazeného v produktu Obrázek 20 na stránce 336 společně s podobným souborem pro CA2, imaginárním certifikačním úřadem, který je nastaven organizací PKI, také v rámci IBM.



Obrázek 21. Příklad struktury informačního stromu adresáře LDAP

Produkt IBM MQ kontroluje seznamy CRL i ARL.

Poznámka: Ujistěte se, že seznam přístupových práv pro váš server LDAP umožňuje autorizovaným uživatelům číst, vyhledávat a porovnávat záznamy, které obsahují seznamy CRL a ARL. Produkt IBM MQ přistupuje k serveru LDAP pomocí vlastností LDAPUSER a LDAPPWD objektu AUTHINFO.

Konfigurace a aktualizace serverů LDAP
Tento postup použijte ke konfiguraci nebo aktualizaci vašeho serveru LDAP.

1. Získejte seznamy CRL a ARL ve formátu DER od certifikačních autorit nebo oprávnění.
2. Pomocí textového editoru nebo nástroje, který jste obdrželi se serverem LDAP, vytvořte jeden nebo více souborů LDIF, které obsahují rozlišující název certifikační autority a požadované definice třídy objektů. Zkopírujte data formátu DER do souboru LDIF jako hodnoty atributu `certificateRevocationList;binary` pro CRL, atribut `authorityRevocationList;binary` pro ARLs, nebo obojí.
3. Spusťte server LDAP.
4. Přidejte položky ze souboru LDIF nebo souborů, které jste vytvořili v kroku “2” na stránce 336.

Po konfiguraci serveru LDAP CRL zkontrolujte, zda je správně nastaven. Nejprve zkuste použít certifikát, který není na kanálu odvolán, a zkontrolujte, zda se kanál spouští správně. Pak použijte certifikát, který je zrušený, a zkontrolujte, zda se kanál nespustí.

Často si vyžádejte aktualizované seznamy CRL od certifikačních autorit. Zvažte to na vašich serverech LDAP každých 12 hodin.

Přístup k seznačkám CRL a ARL se správcem front

Správce front je přidružen k jednomu nebo více objektům ověřovacích informací, které uchovávají adresu serveru LDAP CRL. IBM i IBM MQ na IBM i se chová jinak než ostatní platformy.

Všimněte si, že v této sekci se informace o seznamech CRL (Certificate Revocation Lists) vztahují také na seznamy odvolaných autorit (ARLs).

Správci front sděáte, jak přistupovat k seznamu CRL, zadáním správce front s objekty ověřovacích informací, z nichž každý uchovává adresu serveru LDAP CRL. Objekty ověřovacích informací se nacházejí v seznamu názvů, který je zadán v atributu správce front *SSLCRLNL* .

V následujícím příkladu se používá MQSC pro uvedení parametrů:

1. Definujte objekty ověřovacích informací pomocí příkazu DEFINE AUTHINFO MQSC s parametrem AUTHTYPE nastaveným na CRLLDAP. IBM i V systému IBM imůžete také použít příkaz CL CRTMQMAUTI.

   Hodnota CRLLDAP pro parametr AUTHTYPE indikuje, že k seznamavám 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, servery LDAP, na které odkazují, musí obsahovat stejné informace. Tato funkce zajišťuje kontinuitu služby, pokud selže jeden nebo více serverů LDAP.

   z/OS Navíc, pouze v systému z/OS musí být přístup ke všem serverům LDAP používán se stejným ID uživatele a heslem. Použité ID uživatele a heslo jsou uvedeny v prvním objektu AUTHINFO v seznamu názvů.

   Na všech platformách se ID uživatele a heslo posílají na server LDAP nešifrovaně.
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 hodnotu AUTHINFO.
3. Pomocí příkazu ALTER QMGR MQSC zadejte seznam názvů do správce front. Příklad:

   ```
   ALTER QMGR SSLCRLNL(sslcrlnlname)
   ```

   kde `sslcrlnlname` je váš seznam názvů objektů ověřovacích informací.

   Tento příkaz nastavuje 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 IBM MQ klienti používající tabulku připojení klienta vygenerovanou správcem front produktu IBM i používají informace o ověření určené pro daného správce front IBM i . Atribut správce front *SSLCRLNL* na systému IBM i určuje, jaké informace o ověření používají klienti. See “Přístup k seznačkám CRL a ARL v systému IBM i” na stránce 337 for information about telling an IBM i queue manager how to access CRLs.

Do seznamu názvů můžete přidat až 10 připojení k alternativním serverům LDAP, abyste zajistili nepřetržitost služby, pokud selže jeden nebo více serverů LDAP. Všimněte si, že servery LDAP musí obsahovat identické informace.

IBM i *Přístup k seznačkám CRL a ARL v systému IBM i*

Tuto proceduru použijte pro přístup k CRL nebo ARL na IBM i.

Všimněte si, že v této sekci se informace o seznamech CRL (Certificate Revocation Lists) vztahují také na seznamy odvolaných autorit (ARLs).

Chcete-li nastavit umístění CRL pro určitý certifikát na systému IBM i, postupujte takto:

1. Přistupte k rozhraní DCM, jak je popsáno v tématu “Přístup k DCM” na stránce 268.
2. V kategorii úloh **Správa umístění CRL** v navigačním panelu klepněte na volbu **Přidat umístění CRL**. Stránka Správa umístění CRL se zobrazí v rámci úlohy.
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 zabezpečení SSL (Secure Sockets Layer)** vyberte volbu **Ano** , chcete-li se připojit k serveru LDAP pomocí TLS. V opačném případě vyberte volbu **Ne**.
6. Do pole **Číslo portu** zadejte číslo portu pro server LDAP, například 389.
7. Pokud váš server LDAP neumožňuje anonymním uživatelům zadávat dotazy na adresář, zadejte přihlašovací rozlišující název serveru do pole **Přihlašovací rozlišující název** .
8. Klepněte na tlačítko **OK**. Produkt DCM vás informuje o tom, že vytvořil umístění CRL.
9. V navigačním panelu klepněte na **Výběr úložiště certifikátů**. V rámci úlohy se zobrazí stránka Výběr úložiště certifikátů.
10. Označte zaškrtávací políčko **Další systémové úložiště certifikátů** a klepněte na **Pokračovat**. Zobrazí se stránka Paměť certifikátů a heslo.
11. V poli **Cesta k úložišti certifikátů a název souboru** zadejte cestu k souboru IFS a název souboru, který jste nastavili při “Vytvoření úložiště certifikátů v systému IBM i” na stránce 269.
12. Do pole **Heslo úložiště certifikátů** zadejte heslo. Klepněte na tlačítko **Pokračovat**. V rámci úlohy se zobrazí stránka Aktuální úložiště certifikátů.
13. V kategorii úloh **Správa certifikátů** 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 CRL. Klepněte na **Aktualizace přiřazení umístění CRL**. Stránka Aktualizace přiřazení umístění CRL se zobrazí v rámci úlohy.
15. Vyberte přepínač pro umístění CRL, které chcete přiřadit k certifikátu. Klepněte na tlačítko **Aktualizovat přiřazení**. Produkt DCM vás informuje o tom, že aktualizoval přiřazení.

Všimněte si, že produkt DCM vám umožňuje přiřadit jiný server LDAP certifikačním úřadem.

Přístup k seznačkám CRL a ARL pomocí produktu IBM MQ Explorer
Pomocí produktu IBM MQ Explorer můžete správci front sdělit, jak přistupovat k seznamu odvolaných certifikátů (CRL).

Všimněte si, že v této sekci se informace o seznamech CRL (Certificate Revocation Lists) vztahují také na seznamy odvolaných autorit (ARLs).

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 poté klepněte na volbu **Nový-> Ověřovací informace**. V listu vlastností, který se otevře:
   a. Na první stránce **Vytvořit ověřovací informace**zadejte název pro objekt CRL (LDAP).
   b. Na stránce **Obecné** ve volbě **Změnit vlastnosti**vyberte typ připojení. Volitelně můžete zadat popis.
   c. Vyberte stránku **Seznam CRL (LDAP)** v části **Změnit vlastnosti**.
   d. Zadejte název serveru LDAP buď jako název sítě, nebo jako adresu IP.
   e. Vyžaduje-li server podrobnosti přihlášení, zadejte ID uživatele a v případě potřeby heslo.
   f. Klepněte na tlačítko **OK**.
3. Klepněte pravým tlačítkem myši na složku seznamu názvů a poté 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 338) do seznamu.

c. Klepněte na tlačítko **OK**.

4. Klepněte pravým tlačítkem myši na správce front, vyberte volbu **Vlastnosti**a poté vyberte stránku **SSL** :
   a. Vyberte zaškrtávací políčko **Zkontrolovat certifikáty přijaté tímto správcem front proti seznamům odvolaných certifikátů** .
   b. Zadejte název seznamu názvů (z kroku “3.a” na stránce 338) v poli **Seznam názvů CRL** .

Přístup k seznačkám CRL a ARL s IBM MQ MQI client

K dispozici jsou tři možnosti určení serverů LDAP, které obsahují seznamy CRL pro kontrolu pomocí produktu IBM MQ MQI client.

Všimněte si, že v této sekci se informace o seznamech CRL (Certificate Revocation Lists) vztahují také na seznamy odvolaných autorit (ARLs).

Tři způsoby určení serverů LDAP jsou následující:

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

Další podrobnosti naleznete v souvisejících informacích.

Můžete zahrnout až 10 připojení k alternativním serverům LDAP, abyste zajistili nepřetržitost služby, pokud selže jeden nebo více serverů LDAP. Všimněte si, že servery LDAP musí obsahovat identické informace.

Nelze přistupovat k seznam CRL LDAP z kanálu produktu IBM MQ MQI client spuštěného na platformě Linux (platforma zSeries).

Umístění odpovídacího modulu OCSP a serverů LDAP, které obsahují seznamy odvolaných certifikátů (CRL)
V systému IBM MQ MQI client můžete zadat umístění odpovídacího modulu OCSP a serverů LDAP (Lightweight Directory Access Protocol), které uchovávají seznamy zrušených certifikátů (CRL).

Tato umístění můžete určit třemi způsoby, jak je popsáno zde, v pořadí klesající priority.

IBM i Informace o produktu IBM inajdete v tématu Přístup k seznačkám 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 uchovává seznamy odvolaných certifikátů při volání **MQCONNX** .

Na volání příkazu **MQCONNX** se struktura voleb připojení MQCNO může odkazovat na strukturu voleb konfigurace SSL, MQSCO. Struktura MQSCO se dále může odkazovat na jednu nebo více struktur záznamů ověřovacích informací, MQAIR. Každá struktura MQAIR obsahuje všechny informace, které produkt IBM MQ MQI client potřebuje pro přístup k odpovídacímu modulu OCSP nebo k serveru LDAP s holdkami CRL. Například jedno z polí ve struktuře MQAIR je adresa URL, na které lze kontaktovat odpovídací modul. Další informace o struktuře MQAIR naleznete v tématu Záznam aplikace MQAIR-Authentication.

Přístup k odpovídacímu modulu OCSP nebo serverům LDAP pomocí tabulky definic kanálů klienta (ccdt).

Takže produkt IBM MQ MQI client může přistupovat k odpovídacímu modulu OCSP nebo serverům LDAP, které obsahují seznamy CRL, obsahují atributy jednoho nebo více objektů ověřovacích informací v tabulce definic kanálů klienta.

Na správci front serveru můžete definovat jeden nebo více objektů ověřovacích informací. Atributy objektu ověření obsahují všechny informace, které jsou vyžadovány pro přístup k odpovídacímu modulu OCSP (na platformách, kde je protokol OCSP podporován), nebo na serveru LDAP, který obsahuje seznamy

odvolaných certifikátů (CRL). Jeden z atributů uvádí adresu URL odpovídacího modulu OCSP, další uvádí adresu hostitele nebo adresu IP systému, na kterém je spuštěn server LDAP.

z/OS IBM i Objekt ověřovacích informací s typem AUTHTYPE (OCSP) se nepoužívá pro použití ve správcích front IBM i nebo z/OS , ale lze jej zadat na těchto platformách, které mají být zkopírované do tabulky definic kanálů klienta (CCDT) pro klientské použití.

Chcete-li produktu IBM MQ MQI client povolit přístup k odpovídacímu modulu OCSP nebo serverům LDAP, které obsahují seznamy odvolaných certifikátů, mohou být atributy jednoho nebo více objektů ověřovacích informací zahrnuty do definiční tabulky kanálu klienta. Takové atributy můžete zahrnout do jednoho 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, může být konfigurován více než jeden server LDAP, aby poskytoval vyšší dostupnost. Záměrem je, aby každý server LDAP udržující stejné seznamy CRL. Pokud je jeden server LDAP nedostupný, když je tento server požadován, může se IBM MQ MQI client pokusit o přístup k jinému.

Atributy objektů ověřovacích informací, které jsou identifikovány v seznamu názvů, jsou souhrnně označovány jako *umístění odvolaných certifikátů*. Když nastavíte atribut správce front **SSLCRLNL**na název seznamu názvů, bude umístění odvolaných certifikátů (CRL) zkopírováno do tabulky definic kanálů klienta přidružené ke správci front. Pokud lze k tabulce CCDT přistupovat z klientského systému jako sdíleného souboru, nebo pokud je tabulka CCDT poté zkopírována do systému klienta, může produkt IBM MQ MQI client v daném systému používat umístění odvolaných certifikátů v tabulce CCDT k přístupu k odpovídacímu modulu OCSP nebo serverům LDAP, které obsahují seznamy CRL.

Je-li umístění odvolání certifikátu správce front změněno později, změna se projeví v tabulce CCDT přidružené ke správci front. Je-li atribut správce front **SSLCRLNL**nastaven na prázdnou hodnotu, bude umístění odvolaných certifikátů odebráno z tabulky CCDT. Tyto změny se neprojeví v žádné kopii tabulky na klientském systému.

Požadujete-li umístění odvolání certifikátu na straně klienta a serveru pro jiný kanál MQI a správce front serveru se používá k vytvoření umístění odvolaných certifikátů, můžete následujícím způsobem provést následující akce:

1. Na správci front serveru vytvořte umístění odvolaných certifikátů pro použití v systému klienta.
2. Zkopírujte tabulky CCDT obsahující umístění odvolaných certifikátů do systému klienta.
3. Ve správci front serveru změňte umístění odvolání certifikátů na to, co je povinné na serveru kanálu MQI na serveru.
4. Na klientském počítači můžete použít příkaz **runmqsc** s parametrem **-n** .

Multi

Na platformách klienta AIX, Linux, IBM ia Windows

CCDT můžete sestavit na klientském počítači pomocí příkazu runmqsc s parametry **-n** a **DEFINE AUTHINFO** objekty v souboru CCDT. Pořadí, ve kterém jsou objekty definovány, je pořadí, ve kterém se tyto objekty používají v souboru. Jakýkoliv název, který můžete použít v objektu **DEFINE AUTHINFO** , není uchován v souboru. Při **DISPLAY** objektech **AUTHINFO** v souboru CCDT se používají pouze poziční čísla.

Poznámka: Pokud zadáte argument **-n** , nesmíte zadat žádný jiný parametr.

Použití Active Directory na systému Windows

Windows

Na systémech Windows můžete použít řídicí příkaz **setmqcrl** k publikování aktuálních informací o seznamu CRL v adresáři Active Directory.

Příkaz **setmqcrl** nezveřejňuje informace OCSP.

Informace o tomto příkazu a jeho syntaxi naleznete v souboru setmqcrl.

Přístup k seznačkám CRL a ARL s IBM MQ classes for Java a IBM MQ classes for JMS

IBM MQ classes for Java a IBM MQ classes for JMS přistupují k seznavám CRL jinak než na jiných platformách.

Informace o práci s seznamy CRL a ARL pomocí produktu IBM MQ classes for Javanaleznete v tématu Použití seznamů odvolaných certifikátů .

Informace o práci s seznamy CRL a ARL pomocí produktu IBM MQ classes for JMSviz vlastnost objektu SSLCERTSTORES

Manipulace s objekty ověřovacích informací

Objekty ověřovacích informací můžete manipulovat pomocí příkazů MQSC nebo PCF, nebo pomocí IBM MQ Explorer.

Následující příkazy MQSC pracují na objektech ověřovacích informací:

- DEFINOVAT AUTHINFO
- ZMĚNIT AUTHINFO
- ODSTRANIT AUTHINFO
- ZOBRAZIT AUTHINFO

Úplný popis těchto příkazů najdete v tématu Příkazy MQSC.

Následující příkazy Programmable Command Format (PCF) pracují 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 najdete v tématu Definice formátů Programovatelných příkazů.

Na platformách, kde je k dispozici, můžete použít také produkt IBM MQ Explorer.

Linux AIX Použití metody PAM (Pluggable Authentication Method)

Modul PAM lze používat pouze na platformách AIX and Linux . Typický systém AIX nebo Linux má moduly PAM, které implementují tradiční mechanizmus ověřování, avšak mohou existovat i další. Stejně jako základní úloha ověření platnosti hesel lze také vyvolat moduly PAM k provedení dalších pravidel.

Konfigurační soubory definují, která metoda ověření má být použita pro každou aplikaci. Příklady aplikací zahrnují standardní přihlášení terminálu, ftp a telnet.

Výhodou modulu PAM je to, že aplikace nemusí vědět o skutečnosti, jak se ID uživatele skutečně ověřuje. Pokud aplikace může poskytovat správný formulář ověřovacích dat na PAM, je tento mechanismus za sebou transparentní.

Forma ověřovacích dat závisí na použitém systému. Například produkt IBM MQ získá heslo prostřednictvím parametrů, jako je struktura MQCSP použitá ve volání rozhraní API produktu MQCONNX .

Důležité: Nemůžete nastavit atribut **AUTHENMD** , dokud nenainstalujete produkt IBM MQ 8.0.0 Fix Pack 3, a pak restartujte správce front pomocí **-e CMDLEVEL=***úrovně* z *802* (v příkazu strmqm), abyste nastavili úroveň příkazů, kterou požadujete.

Konfigurace systému pro použití modulu PAM

Název služby použitý produktem IBM MQpři vyvolání modulu PAM je *ibmmq*.

Všimněte si, že instalace produktu IBM MQ se pokouší zachovat výchozí konfiguraci PAM, která povoluje připojení od uživatelů operačního systému, založená na známých výchozích hodnotách pro různé operační systémy.

Administrátor systému však musí ověřit, zda jsou pravidla definovaná v produktu `/etc/pam.conf`nebo `/etc/pam.d/ibmmq`, soubory stále odpovídající.

Autorizace přístupu k objektům

Tento oddíl obsahuje informace o používání správce oprávnění k objektu a ukončovacích programů kanálu k řízení přístupu k objektům.

ALW V systémech AIX, Linux, and Windows . řízením přístupu k objektům můžete řídit pomocí správce oprávnění k objektu (OAM). Tato kolekce témat obsahuje informace o použití příkazového rozhraní pro OAM.

Tato sekce také obsahuje kontrolní seznam, který můžete použít k určení úloh, které mají být provedeny, na zabezpečení systému na všech platformách a pokyny pro udělení oprávnění uživatelům k administraci produktu IBM MQ a práci s objekty produktu IBM MQ .

Pokud dodané bezpečnostní mechanismy nevyhovují vašim potřebám, můžete vyvinout vlastní uživatelské programy 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.

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 342 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 68. 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 v systému AIX, Linux, and Windows

Správce oprávnění k objektu (OAM) poskytuje příkazové rozhraní pro udělování a odebírání oprávnění k objektům produktu IBM MQ .

Musíte být vhodně autorizováni pro použití těchto příkazů, jak je popsáno v "Oprávnění ke správě produktu IBM MQ v systému AIX, Linux, and Windows" na stránce 391. ID uživatele, která jsou autorizována pro administraci produktu IBM MQ , mají oprávnění *superuživatele* ke správci front, což znamená, že jim nemusíte udělit další oprávnění k vydávání jakýchkoli požadavků nebo příkazů MQI.

Linux AIX Oprávnění pro uživatele OAM v systému AIX and Linux

V systému IBM MQ 8.0v systémech UNIX and Linux může správce oprávnění k objektu (OAM) používat autorizaci založenou na uživateli a autorizaci založenou na skupinách.

Před IBM MQ 8.0jsou seznamy přístupových práv (ACL) na UNIX and Linux založeny pouze na skupinách. V produktu IBM MQ 8.0jsou seznamy ACL založeny na identifikátorech uživatelů a skupinách a můžete použít buď model založený na uživateli, nebo skupinový model pro autorizaci nastavením atributu **SecurityPolicy** na příslušnou hodnotu podle popisu v části Konfigurace instalovatelných služeb a Konfigurace stanzy autorizační služby v systému AIX and Linux.

Změny v chování pro produkt IBM MQ 8.0 a novější

V případě produktu IBM MQ 8.0, pokud je spuštěn s uživatelskou zásadou, některé příkazy vrací různé informace ze starších verzí 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 uživateli.
- Funkce OAM **Inquire** vrací výsledky, které ukazují, že je to možné uživatele.

Použití atributu **-p** v příkazu **setmqaut** neuděluje přístup všem uživatelům ve stejné primární skupině, jsou-li autorizace založené na uživateli povoleny v souboru `qm.ini` , jak je popsáno ve stanze Service stanza souboru qm.ini.

Pokud začínáte používat autorizaci založenou na uživateli a mít mnoho uživatelů, bude pravděpodobně více záznamů, které jsou uloženy ve frontě AUTH než s modelem založeným na skupině, a proces autorizace může trvat o něco déle než dříve, protože je k dispozici více záznamů k ověření. Toto zvýšení se nepředpokládá, že by bylo významné. Je-li to nutné, můžete použít kombinaci oprávnění uživatele a skupiny.

Aspekty migrace

Změníte-li model ze skupiny na uživatele existujícího správce front, nedojde k okamžitému použití. Oprávnění, která již byla provedena, se budou nadále používat. Jakýkoli uživatel, který se připojí ke správci front, obdrží stejná oprávnění jako předtím: kombinace všech skupin, do kterých patří jejich ID. Když jsou pro ID uživatelů vydány nové příkazy **setmqaut** , mají okamžitý účinek.

Pokud vytváříte nového správce front s touto zásadou uživatele, má tento správce front oprávnění pouze pro uživatele, který jej vytvořil (což je obvykle, ale ne nezbytně, ID uživatele `mqm`). Existují také oprávnění, která jsou automaticky udělena skupině `mqm` . Pokud však nemáte roli `mqm` jako primární skupinu, nebude skupina `mqm` zahrnuta do počáteční sady oprávnění.

Pokud se přesunete od uživatele do skupiny zásad, autorizace založené na uživateli se automaticky neodstraní. Avšak během kontroly oprávnění se již nepoužívají. Před opětovným vrácením této zásady uložte aktuální konfiguraci, změňte zásadu, restartujte správce front a poté skript znovu spusťte. Vzhledem k tomu, že se nyní jedná o správce front na základě skupiny, je tento efekt uložen na základě primární skupiny, která je uložena na základě primární skupiny.

Související pojmy

správce oprávnění k objektu (OAM)

Činitelé a skupiny v systémech UNIX, Linux a Windows

Sekce Service souboru qm.ini

Související odkazy

Příkaz **crtmqm** (vytvoření správce front)

ALW Udělení přístupu k objektu IBM MQ v systému AIX, Linux, and Windows

Pomocí řídicího příkazu **setmqaut** , příkazu **SET AUTHREC** MQSC nebo příkazu **MQCMD_SET_AUTH_REC** PCF udělte přístup k objektům IBM MQ uživatelům a skupinám uživatelů. Všimněte si, že v produktu IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Úplnou definici řídicího příkazu **setmqaut** a jeho syntaxi naleznete v části setmqaut.

Úplnou definici příkazu MQSC **SET AUTHREC** a jeho syntaxi naleznete v části SET AUTHREC.

Úplnou definici příkazu **MQCMD_SET_AUTH_REC** PCF a jeho syntaxi naleznete v tématu Nastavení záznamu oprávnění.

Aby bylo možné použít tento příkaz, musí být spuštěn správce front. Pokud jste změnili přístup pro činitele, změny se projeví okamžitě u OAM.

Chcete-li udělit uživatelům přístup k objektu, je třeba určit:

- Název správce front, který je vlastníkem objektů, se kterými pracujete. Pokud nezadáte název správce front, bude předpokládán výchozí správce front.
- Název a typ objektu (pro jednoznačnou identifikaci objektu). Zadejte název jako *profil* . to je 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 346.
- Jeden nebo více názvů činitelů a skupin, na které se oprávnění vztahuje.

  Pokud ID uživatele obsahuje mezery, uzavřete jej do uvozovek, když použijete tento příkaz. V systému Windows můžete kvalifikovat ID uživatele s názvem domény. Pokud skutečné jméno uživatele obsahuje znak zavináč (@), nahraďte jej znakem @ @ a zobrazí se, že je součástí ID uživatele, nikoli pomocí oddělovače mezi ID uživatele a názvem domény.
- Seznam autorizací. Každá položka v seznamu uvádí typ přístupu, který má být udělen tomuto objektu (nebo mu bylo odebráno). Každá autorizace v seznamu je uvedena jako klíčové slovo, předpona se znaménkem plus (+) nebo znaménka minus (-). Chcete-li přidat zadané oprávnění, použijte znaménko plus a pomocí znaku minus odeberte autorizaci. Mezi znakem + nebo-znakem a klíčovým slovem nesmí být žádné mezery.

  V jednom příkazu můžete zadat libovolný počet autorizací. Například seznam autorizací, které umožňují uživateli nebo skupině vkládat zprávy do fronty a procházet je, ale zrušit přístup k získání zpráv je následující:

```
+browse -get +put
```

Příklady použití příkazu setmqaut

Následující příklady ukazují, jak použít příkaz `setmqaut` k udělení a odebrání 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
  - `+browse` přidá autorizaci k procházení zpráv ve frontě (chcete-li vydat příkaz **MQGET** s volbou procházení)
  - `-get` odstraní autorizaci k získání zpráv (**MQGET**) z fronty
  - `+put` přidává oprávnění k vkládání zpráv (**MQPUT**) do fronty

Následující příkaz odvolá oprávnění k vložení do fronty MyQueue od činitele fvuser a ze skupiny grouppa a groupb. U systémů AIX and Linux tento příkaz také odvolá oprávnění k vložení pro všechny činitele ve stejné primární skupině jako uživatel 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 používáte vlastní autorizační službu místo OAM, můžete uvést název této služby na příkaz **setmqaut** , abyste přesměli příkaz na tuto službu. Tento parametr musíte určit, máte-li současně spuštěné více instalovatelných komponent. Pokud tuto aktualizaci nepoužíváte, provede se aktualizace na první instalovatelnou komponentu pro autorizační službu. Ve výchozím nastavení je to dodaný 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.JKL`a `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.JKL`a `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 v systému AIX, Linux, and Windows*

Použijte zástupné znaky v názvu profilu OAM (Object Authority Manager), abyste učinili tento profil použitelný pro více než jeden objekt.

Co znamená, že generický profil je použití speciálních znaků (zástupné znaky) v názvu profilu. Zástupný znak otazníku (?) se například shoduje s libovolným znakem v názvu. Pokud tedy zadáte `ABC.?EF`, autorizace, kterou poskytnete tomuto profilu, se vztahuje na všechny objekty s názvy `ABC.DEF`, `ABC.CEF`, `ABC.BEF`atd.

Dostupné zástupné znaky jsou:

?

Otazník (?) zastupuje libovolný jeden znak. Například `AB.?D` se vztahuje na objekty `AB.CD`, `AB.ED`a `AB.FD`.

*****

Použijte hvězdičku (*) jako:

- *Kvalifikátor* v názvu profilu, který odpovídá 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` se vztahuje na objekty `ABC.DEF.JKL`a `ABC.GHI.JKL`. (Všimněte si, že se **nevztahuje** na `ABC.JKL` ; * použitý v tomto kontextu vždy označuje jeden kvalifikátor.)
- Znak uvnitř kvalifikátoru v názvu profilu, který odpovídá žádnému znaku nebo více znakům v rámci kvalifikátoru ve jménu objektu.

  Například `ABC.DE*.JKL` se vztahuje na objekty `ABC.DE.JKL`, `ABC.DEF.JKL`a `ABC.DEGH.JKL`.

******

Použijte dvojitá hvězdička (**) **jednou** v názvu profilu jako:

- Celý název profilu, který odpovídá všem názvům objektů. Pokud například používáte produkt `-t prcs` k identifikaci procesů, použijte jako název profilu volbu **, změníte oprávnění pro všechny procesy.
- Jako počáteční, střední nebo koncový kvalifikátor v názvu profilu odpovídá jednomu 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 v systému AIX, Linux, and Windows*

Na jeden objekt může být použit více než jeden generický profil. Pokud se jedná o tento případ, použije se nejspecifičtější pravidlo.

Důležitým bodem pro pochopení použití generických profilů je priorita, která jsou při rozhodování o tom, jaká oprávnění mají být použita na vytvářený objekt, upřednostňována. Předpokládejme například, že jste tyto příkazy zadali:

```
setmqaut -n AB.* -t q +put -p fred
setmqaut -n AB.C* -t q +get -p fred
```

První dává oprávnění ke všem frontám pro činitele fred s názvy, které odpovídají profilu AB. *; druhý dává oprávnění ke stejným typům front, které odpovídají profilu AB.C*.

Předpokládejme, že nyní vytvoříte frontu s názvem AB.CD. Podle pravidel pro hledání shody se zástupnými znaky může být u této fronty použit příkaz setmqaut. Takže, má to dát nebo získat oprávnění?

Chcete-li najít odpověď, aplikujete pravidlo, které, kdykoli se může na objekt použít více profilů, **pouze nejspecifičtější použití**. Způsob použití tohoto pravidla je porovnáváním názvů profilů zleva doprava. Kamkoli se liší, negenerický znak je spíše specifický než generický znak. Takže, v tomto příkladu, fronta AB.CD má autoritu **get** (AB.C* je více specifická než AB. *).

Porovnáváte-li generické znaky, pořadí *specifičnosti* je:

1. ?
2. *
3. **

Viz SET AUTHREC pro ekvivalentní informace při použití tohoto příkazu MQSC.

ALW *Výpis nastavení profilu v systému AIX, Linux, and Windows*

Chcete-li vypsat aktuální autorizace přidružené k určenému profilu, použijte řídicí příkaz **dmpmqaut** , příkaz MQSC **DISPLAY AUTHREC** nebo příkaz **MQCMD_INQUIRE_AUTH_RECS** PCF. Všimněte si, že v produktu IBM MQ Appliance můžete použít pouze příkaz **DISPLAY AUTHREC** .

Úplnou definici řídicího příkazu **dmpmqaut** a jeho syntaxi naleznete v popisu příkazu dmpmqaute.

Úplnou definici příkazu MQSC **DISPLAY AUTHREC** a jeho syntaxi naleznete v příručce DISPLAY AUTHREC.

Úplnou definici příkazu **MQCMD_INQUIRE_AUTH_RECS** PCF a její syntaxi naleznete v tématu Inquire Authority Records.

Následující příklady ukazují použití obslužného 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 bude vypadat podobně jako v tomto příkladu:

   ```
   profile:     a.b.*
   object type: queue
   entity:      user1
   type:        principal
   authority:   get, browse, put, inq
   ```

   Poznámka: Uživatelé AIX and Linux nemohou použít volbu `-p` ; místo toho musí 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 bude vypadat 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. *, fronty typu.

   ```
   dmpmqaut -m qmgr1 -n a.b.* -t q
   ```

   Výsledný výpis bude vypadat 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 bude vypadat 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 bude vypadat 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 řídicí služby 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 v systému AIX, Linux, and Windows

Použijte řídicí příkaz **dspmqaut** , příkaz **DISPLAY AUTHREC** MQSC nebo příkaz **MQCMD_INQUIRE_ENTITY_AUTH** PCF pro zobrazení autorizací, které určitý činitel nebo skupina má pro konkrétní objekt. Všimněte si, že v produktu IBM MQ Appliance můžete použít pouze příkaz **DISPLAY AUTHREC** .

Aby bylo možné použít tento příkaz, musí být spuštěn správce front. Když změníte přístup pro činitele, změny se projeví okamžitě u OAM. Oprávnění lze v daném okamžiku zobrazit pouze pro jednu skupinu nebo činitele.

Úplnou definici řídicího příkazu **dmpmqaut** a jeho syntaxi naleznete v popisu příkazu dmpmqaute.

Úplnou definici příkazu MQSC **DISPLAY AUTHREC** a jeho syntaxi naleznete v příručce DISPLAY AUTHREC.

Úplnou definici příkazu **MQCMD_INQUIRE_AUTH_RECS** PCF a její syntaxi naleznete v tématu Inquire Authority Records.

Následující příklad zobrazuje použití řídicího příkazu **dspmqaut** k zobrazení autorizací, které má skupina GpAdmin k definici procesu s názvem Annuities , která je 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, kterou má uživatel nebo skupina k objektu, použijte řídicí příkaz **setmqaut** , příkaz **DELETE AUTHREC** MQSC nebo příkaz **MQCMD_DELETE_AUTH_REC** PCF. MQ Appliance Všimněte si, že v produktu 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 141
- AIX "Vytvoření a správa skupin v systému AIX" na stránce 140
- Linux "Vytvoření a správa skupin v systému Linux" na stránce 141

.

ID uživatele, který vytvoří objekt IBM MQ , má k tomuto objektu přiděleno celé oprávnění k řízení. Odeberete-li toto ID uživatele z lokální skupiny mqm (nebo skupiny administrátorů v systému Windows), nebudou tato oprávnění odvolána. Použijte řídicí příkaz **setmqaut** nebo příkaz **MQCMD_DELETE_AUTH_REC** PCF k odvolání přístupu k objektu pro ID uživatele, který jej vytvořil, poté, co jste jej odebrali ze skupiny mqm nebo Administrátoři.

Úplnou definici příkazu řídicího příkazu setmqaut a jeho syntaxi naleznete v části setmqaut.

Úplnou definici příkazu MQSC **DELETE AUTHREC** a jeho syntaxi naleznete v části DELETE AUTHREC.

Úplnou definici příkazu **MQCMD_DELETE_AUTH_REC** PCF a její syntaxi naleznete v tématu Odstranit záznam oprávnění.

Windows V produktu Windowsmůžete v produktu IBM MQ 8.0odstranit položky OAM odpovídající konkrétnímu uživatelskému účtu produktu Windows při použití parametru **-u** *SID* **setmqaut**.

Prior to IBM MQ 8.0, you had to delete the OAM entries corresponding to a particular Windows user account before deleting the user profile. Nebylo možné odebrat položky OAM po odebrání uživatelského účtu.

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 MQSNOAUT a způsobu nastavení MQSNOAUT v systému 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 úlohy

Konfigurace instalovatelných služeb

Související odkazy

Instalovatelné služby a komponenty pro systémy UNIX, Linux a Windows

Referenční informace o instalovatelných službách

Udělení požadovaného přístupu k prostředkům

Prostřednictvím tohoto tématu můžete určit, které úlohy mají být provedeny při použití zabezpečení ve vašem systému IBM MQ .

Informace o této úloze

Během této úlohy rozhodujete o tom, jaké akce jsou nezbytné k použití odpovídající úrovně zabezpečení na prvky vaší instalace produktu IBM MQ . Každá jednotlivá úloha, na kterou jste se odkazujete, poskytuje instrukce po krocích pro všechny platformy.

Postup

1. Potřebujete omezit přístup k vašemu správci front některým uživatelům?
   a) Ne: neprovádět žádnou další akci.
   b) Ano: Přejděte na další otázku.
2. Potřebují tito uživatelé částečný administrativní přístup k podmnožině prostředků správce front?
   a) Ne: Přejděte na další otázku.
   b) Ano: Viz “Udělení částečného administrativního přístupu k podmnožině prostředků správce front” na stránce 355.
3. Potřebují tito uživatelé úplný administrativní přístup k podmnožině prostředků správce front?
   a) Ne: Přejděte na další otázku.
   b) Ano: Viz “Udělení úplného administrativního přístupu k podmnožině prostředků správce front” na stránce 363.
4. Mají tito uživatelé přístup jen pro čtení ke všem prostředkům správce front?
   a) Ne: Přejděte na další otázku.
   b) Ano: Viz “Udělení přístupu jen pro čtení ke všem prostředkům ve správci front” na stránce 370.
5. Potřebují tito uživatelé úplný administrativní přístup ke všem prostředkům správce front?
   a) Ne: Přejděte na další otázku.
   b) Ano: Viz “Udělení úplného administrativního přístupu ke všem prostředkům ve správci front” na stránce 371.
6. Potřebujete uživatelské aplikace pro připojení k vašemu správci front?
   a) Ne: Zakázat konektivitu, jak je popsáno v “Odebrání konektivity ke správci front” na stránce 372
   b) Ano: Viz “Povolení připojení uživatelských aplikací k vašemu správci front” na stránce 373.

Multi z/OS Udělení částečného administrativního přístupu k podmnožině prostředků správce front

Je třeba, abyste určitým uživatelům poskytli částečný administrativní přístup k některým prostředkům správce front, ale ne ke všem prostředkům správce front. Tuto tabulku použijte k určení akcí, které musíte provést.

Tabulka 69. Udělení částečného administrativního přístupu k podmnožině prostředků správce front

Uživatelé potřebují 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 355 .
Témata	Udělte částečný administrativní přístup k požadovaným tématům, jak je popsáno v tématu “Udělení omezeného administrativního přístupu k některým tématům” na stránce 357 .
Kanály	Udělte částečný administrativní přístup k požadovaným kanálům, jak je popsáno v tématu “Udělení omezeného administrativního přístupu k některým kanálům” na stránce 358
Správce front	Udělte částečný administrativní přístup ke správci front, jak je popsáno v tématu “Udělení omezeného administrativního přístupu ke správci front” na stránce 359 .
Procesy	Udělte částečný administrativní přístup k požadovaným procesům, jak je popsáno v tématu “Udělení omezeného administrativního přístupu k některým procesům” na stránce 360 .
Seznamy názvů	Udělení částečného administrativního přístupu k vyžadovaným seznamům názvů, jak je popsáno v tématu “Udělení omezeného administrativního přístupu k některým seznamům názvů” na stránce 361
Služby	Udělte částečný administrativní přístup k požadovaným službám, jak je popsáno v tématu “Udělení omezeného administrativního přístupu k některým službám” na stránce 362

Udělení omezeného administrativního přístupu k některým frontám

Udělte skupině uživatelů částečnou administrativní přístup k některým frontám ve správci front, do každé skupiny uživatelů, kteří pro ni potřebují obchodní potřeby.

Informace o této úloze

Chcete-li pro některé akce udělit omezený administrativní přístup k některým frontám, použijte příslušné příkazy pro váš operační systém.

Na platformách pro více platforem můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance lze 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 IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(ReqdAction) MQMNAME('
QMgrName ')
```

- z/OS Pro 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 provést ve frontě, 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 povolit uživateli použít příkaz 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 generický profil, pro které chcete změnit autorizace.

  GroupName
  Název skupiny, ke které má být udělen přístup.

  ReqdAction
  Akce, kterou povolujete, aby skupina mohla provést:

  – ALW V systémech AIX, Linux, and Windows libovolná kombinace následujících autorizací: + chg, + clr, + dlt, + dsp. Oprávnění + alladm je ekvivalentní s + chg + clr + dlt + dsp.

  – IBM i V systémech IBM ilibovolná kombinace následujících autorizací: *ADMCHG, *ADMCLR, *ADMDLT, *ADMDSP. Autorizace *ALLADM je ekvivalentní ke všem těmto individuálním autorizacím.

  – z/OS V systému z/OSjedna z hodnot ALTER, CLEAR, DELETE nebo MOVE.

  Poznámka: Udělení + crt pro fronty nepřímo činí uživatele nebo skupinu administrátorem. Nepoužívejte oprávnění + crt, abyste udělili omezený administrativní přístup k některým frontám.

QTYPE

Pro příkaz DISPLAY, jedna z hodnot QUEUE, QLOCAL, QALIAS, QMODEL, QREMOTE nebo QCLUSTER.

Pro jiné hodnoty parametru *ReqdAction*, jedna z hodnot QLOCAL, QALIAS, QMODEL nebo QREMOTE.

Udělení omezeného administrativního přístupu k některým tématům

Udělte přístup k částečnému administrativnímu přístupu k některým tématům ve správci front, a to pro každou skupinu uživatelů, kteří pro ni potřebují obchodní potřeby.

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 pro více platforem můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance lze 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 IBM izadejte tento příkaz:

  ```
  GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*TOPIC) USER(GroupName) AUT(ReqdAction) MQMNAME('
  QMgrName ')
  ```

- z/OS Pro 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 uvedenému tématu. Chcete-li určit, které příkazy MQSC může uživatel provést na daném tématu, 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 povolit uživateli použít příkaz 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 generický profil, pro které chcete změnit autorizace.

GroupName
Název skupiny, ke které má být udělen přístup.

ReqdAction
Akce, kterou povolujete, aby skupina mohla provést:

- ALW V systémech AIX, Linux, and Windows libovolná kombinace následujících autorizací: + chg, + clr, + crt, + dlt, + dsp. + CTRL. Oprávnění + alladm je ekvivalentní s + chg + clr + dlt + dsp.
- IBM i V systému IBM ilibovolná kombinace následujících autorizací: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP, *CTRL. Autorizace *ALLADM je ekvivalentní ke všem těmto individuálním autorizacím.
- z/OS V systému z/OSjedna z hodnot ALTER, CLEAR, DEFINE, DELETE nebo MOVE.

Udělení omezeného administrativního přístupu k některým kanálům

Udělte některým kanálům ve správci front částečný administrativní přístup k některým kanálům, a to pro každou skupinu uživatelů, kteří pro ni budou potřebovat obchodní položku.

Informace o této úloze

Chcete-li některým kanálům pro některé akce udělit omezený administrativní přístup k některým kanálům, použijte příslušné příkazy pro daný operační systém.

Na platformách pro více platforem můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance lze 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 uvedenému kanálu. Chcete-li určit, které příkazy MQSC může uživatel na kanálu provést, 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 povolit uživateli použít příkaz 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 generický profil, pro které chcete změnit autorizace.

GroupName
Název skupiny, ke které má být udělen přístup.

ReqdAction
Akce, kterou povolujete, aby skupina mohla provést:

- ALW V systému AIX, Linux, and Windowsjsou všechny kombinace následujících autorizací: + chg, + clr, + crt, + dlt, + dsp. + ctrl, + ctrlx. Oprávnění + alladm je ekvivalentní s + chg + clr + dlt + dsp.
- IBM i V systémech IBM ilibovolná kombinace následujících autorizací: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP, *CTRL, *CTRLx. Autorizace *ALLADM je ekvivalentní ke všem těmto individuálním autorizacím.
- z/OS V systému z/OSjedna z hodnot ALTER, CLEAR, DEFINE, DELETE nebo MOVE.

Udělení omezeného administrativního přístupu ke správci front

Udělte přístup k částečnému administrativnímu přístupu ke správci front, do každé skupiny uživatelů, kteří pro ni potřebují obchodní potřeby.

Informace o této úloze

Chcete-li udělit omezený administrativní přístup k provádění některých akcí ve správci front, použijte příslušné příkazy pro daný operační systém.

Na platformách pro více platforem můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance lze 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 provést na správci front, 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 povolit uživateli použít příkaz 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 generický profil, pro které chcete změnit autorizace.

GroupName
Název skupiny, ke které má být udělen přístup.

ReqdAction
Akce, kterou povolujete, aby skupina mohla provést:

- ALW V systému AIX, Linux, and Windowsjsou všechny kombinace následujících autorizací: + chg, + clr, + crt, + dlt, + dsp. Oprávnění + alladm je ekvivalentní s + chg + clr + dlt + dsp.

  Ačkoli + set je autorizace MQI a není obvykle považována za administrativně, může udělení + nastavení ve správci front nepřímo vést k úplnému administrativnímu oprávnění. Nepřidělovat + nastavit běžným uživatelům a aplikacím.
- IBM i V systémech IBM ilibovolná kombinace následujících autorizací: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP. Autorizace *ALLADM je ekvivalentní ke všem těmto individuálním autorizacím.

Udělení omezeného administrativního přístupu k některým procesům

Udělte některým procesům ve správci front částečný administrativní přístup k některým procesům, a to pro každou skupinu uživatelů, kteří pro ni potřebují obchodní potřeby.

Informace o této úloze

Chcete-li u některých akcí udělit omezený administrativní přístup k některým procesům, použijte příslušné příkazy pro daný operační systém.

Na platformách pro více platforem můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance lze 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 uvedenému kanálu. Chcete-li určit, které příkazy MQSC může uživatel na kanálu provést, 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 povolit uživateli použít příkaz 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 generický profil, pro které chcete změnit autorizace.

GroupName
Název skupiny, ke které má být udělen přístup.

ReqdAction
Akce, kterou povolujete, aby skupina mohla provést:

- ALW V systému AIX, Linux, and Windowsjsou všechny kombinace následujících autorizací: + chg, + clr, + crt, + dlt, + dsp. Oprávnění + alladm je ekvivalentní s + chg + clr + dlt + dsp.
- IBM i V systémech IBM ilibovolná kombinace následujících autorizací: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP. Autorizace *ALLADM je ekvivalentní ke všem těmto individuálním autorizacím.
- z/OS V systému z/OSjedna z hodnot ALTER, CLEAR, DEFINE, DELETE nebo MOVE.

Udělení omezeného administrativního přístupu k některým seznamům názvů

Udělte některým seznamům názvů ve správci front částečný administrativní přístup k některým seznamům názvů, a to pro každou skupinu uživatelů, kteří pro ni potřebují obchodní potřeby.

Informace o této úloze

Chcete-li udělit omezený administrativní přístup k některým seznamům názvů pro některé akce, použijte příslušné příkazy pro váš operační systém.

Na platformách pro více platforem můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance lze 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 uvedenému seznamu názvů. Chcete-li určit, které příkazy MQSC může uživatel v daném seznamu názvů provést, 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 povolit uživateli použít příkaz 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 generický profil, pro které chcete změnit autorizace.

GroupName
Název skupiny, ke které má být udělen přístup.

ReqdAction
Akce, kterou povolujete, aby skupina mohla provést:

- ALW V systému AIX, Linux, and Windowsjsou všechny kombinace následujících autorizací: + chg, + clr, + crt, + dlt, + ctrl, + ctrlx, + dsp. Oprávnění + alladm je ekvivalentní s + chg + clr + dlt + dsp.
- IBM i V systémech IBM ilibovolná kombinace následujících autorizací: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP, *CTRL, *CTRLX. Autorizace *ALLADM je ekvivalentní ke všem těmto individuálním autorizacím.
- z/OS V systému z/OSjedna z hodnot ALTER, CLEAR, DEFINE, DELETE nebo MOVE.

Udělení omezeného administrativního přístupu k některým službám

Udělte určitým službám ve správci front částečný administrativní přístup k některým službám, a to pro každou skupinu uživatelů, kteří ji potřebují.

Informace o této úloze

Chcete-li některým službám udělit omezený administrativní přístup k některým službám, použijte příslušné příkazy pro váš operační systém. z/OS Všimněte si, že objekty služby neexistují v systému z/OS.

Na platformách pro více platforem můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance lze 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 provést na službě, 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 povolit uživateli použít příkaz 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 generický profil, pro které chcete změnit autorizace.

  GroupName
  Název skupiny, ke které má být udělen přístup.

  ReqdAction
  Akce, kterou povolujete, aby skupina mohla provést:

  – ALW V systémech AIX, Linux, and Windows libovolná kombinace následujících autorizací: + chg, + clr, + crt, + dlt, + ctrl, + ctrlx, + dsp. Oprávnění + alladm je ekvivalentní s + chg + clr + dlt + dsp.

  – IBM i V systémech IBM ilibovolná kombinace následujících autorizací: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP, *CTRL, *CTRLX. Autorizace *ALLADM je ekvivalentní ke všem těmto individuálním autorizacím.

Udělení úplného administrativního přístupu k podmnožině prostředků správce front

Je třeba, abyste určitým uživatelům poskytli úplný administrativní přístup k některým prostředkům správce front, ale ne ke všem prostředkům správce front. Použijte tyto tabulky k určení akcí, které musíte provést.

Tabulka 70. Udělení úplného administrativního přístupu k podmnožině prostředků správce front	
Uživatelé potřebují 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 364 .
Témata	Udělte úplný administrativní přístup k požadovaným tématům, jak je popsáno v tématu “Udělení úplného administrativního přístupu k některým tématům” na stránce 365 .
Kanály	Udělte úplný administrativní přístup k požadovaným kanálům, jak je popsáno v tématu “Udělení úplného administrativního přístupu k některým kanálům” na stránce 366 .
Správce front	Udělte úplný administrativní přístup ke správci front, jak je popsáno v tématu “Udělení úplného administrativního přístupu ke správci front” na stránce 366 .
Procesy	Udělte úplný administrativní přístup k požadovaným procesům, jak je popsáno v tématu “Udělení úplného administrativního přístupu k některým procesům” na stránce 367 .
Seznamy názvů	Udělit úplný administrativní přístup k vyžadovaným seznamům názvů, jak je popsáno v tématu “Udělení úplného administrativního přístupu k některým seznamům názvů” na stránce 368
Služby	Udělte úplný administrativní přístup k požadovaným službám, jak je popsáno v tématu “Udělení úplného administrativního přístupu k některým službám” na stránce 369

Udělení úplného administrativního přístupu k některým frontám

Udělte úplný administrativní přístup k některým frontám ve správci front, do každé skupiny uživatelů, kteří pro ni potřebují obchodní potřeby.

Informace o této úloze

Chcete-li udělit úplný administrativní přístup k některým frontám, použijte příslušné příkazy pro váš operační systém.

Na platformách pro více platforem můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance lze 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 generický profil, pro které chcete změnit autorizace.

  GroupName
  Název skupiny, ke které má být udělen přístup.

Udělení úplného administrativního přístupu k některým tématům

Udělte úplný administrativní přístup k některým tématům ve správci front, do každé skupiny uživatelů, kteří pro ni potřebují obchodní potřeby.

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 pro více platforem můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance lze 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 generický profil, pro které chcete změnit autorizace.

GroupName
Název skupiny, ke které má být udělen přístup.

Udělení úplného administrativního přístupu k některým kanálům

Udělte úplný administrativní přístup k některým kanálům ve správci front, a to pro každou skupinu uživatelů, kteří pro ni potřebují obchodní činnost.

Informace o této úloze

Chcete-li udělit úplný administrativní přístup k některým kanálům, použijte příslušné příkazy pro daný operační systém.

Na platformách pro více platforem můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance lze 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 generický profil, pro které chcete změnit autorizace.

  GroupName
  Název skupiny, ke které má být udělen přístup.

Udělení úplného administrativního přístupu ke správci front

Udělte úplný administrativní přístup ke správci front, do každé skupiny uživatelů, kteří pro ni potřebují obchodní potřeby.

Informace o této úloze

Chcete-li udělit úplný administrativní přístup ke správci front, použijte příslušné příkazy pro váš operační systém.

Na platformách pro více platforem můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance lze 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 generický profil, pro které chcete změnit autorizace.

  GroupName
  Název skupiny, ke které má být udělen přístup.

Udělení úplného administrativního přístupu k některým procesům

Udělte úplný administrativní přístup k některým procesům ve správci front, a to pro každou skupinu uživatelů, kteří pro ni potřebují obchodní činnost.

Informace o této úloze

Chcete-li udělit úplný administrativní přístup k některým procesům, použijte příslušné příkazy pro váš operační systém.

Na platformách pro více platforem můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance lze 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 generický profil, pro které chcete změnit autorizace.

GroupName
Název skupiny, ke které má být udělen přístup.

Udělení úplného administrativního přístupu k některým seznamům názvů

Udělte úplný administrativní přístup k některým seznamům názvů ve správci front, do každé skupiny uživatelů, kteří pro ni potřebují obchodní potřeby.

Informace o této úloze

Chcete-li udělit úplný administrativní přístup k některým seznamům názvů, použijte příslušné příkazy pro váš operační systém.

Na platformách pro více platforem můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance lze 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 generický profil, pro které chcete změnit autorizace.

GroupName
Název skupiny, ke které má být udělen přístup.

Udělení úplného administrativního přístupu k některým službám

Udělte úplný administrativní přístup k některým službám ve správci front, do každé skupiny uživatelů, kteří pro ni potřebují obchodní potřeby.

Informace o této úloze

Chcete-li udělit úplný administrativní přístup k některým službám, použijte příslušné příkazy pro váš operační systém.

Na platformách pro více platforem můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance lze 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 generický profil, pro které chcete změnit autorizace.

GroupName
Název skupiny, ke 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 pro více platforem můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance lze 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, kteří pro ni potřebují obchodní potřeby.

Informace o této úloze

Můžete použít průvodce Přidat oprávnění založená na rolích nebo příslušné příkazy pro váš operační systém.

Na platformách pro více platforem můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance lze použít pouze příkaz **SET AUTHREC** .

Notes: ALW

1. Používáte-li produkt **runmqsc** k administraci správce front místo produktu IBM MQ Explorer, musíte udělit oprávnění k získání, zjišťování a procházení SYSTEM.MQSC.REPLY.QUEUEa vy nemusíte udělovat žádné oprávnění k SYSTEM.MQEXPLORER.REPLY.MODEL fronta.
2. Při poskytnutí přístupu uživatele ke všem prostředkům ve správci front existují některé příkazy, které uživatel nemůže spustit, pokud tento uživatel nemá přístup pro čtení k souboru `qm.ini` . Důvodem je omezení na to, aby uživatelé produktu `mqm` , kteří nejsou schopni číst soubor `qm.ini` , byli schopni číst.

   Uživatel nemůže vydat následující příkazy, pokud jste tomuto uživateli neudělili přístup pro čtení k souboru qm.ini :

   - Definování kanálu, který je konfigurován pro použití TLS
   - Definování kanálu pomocí proměnných vložení s automatickou konfigurací, které jsou definovány v produktu `qm.ini`

Procedura

- Pokud používáte průvodce, klepněte v podokně IBM MQ Explorer Navigator pravým tlačítkem myši na správce front a klepněte na volbu **Oprávnění pro objekty** > **Přidat oprávnění založená na rolích**.

  Otevře se průvodce Přidat oprávnění založená na rolích.
- Linux AIX

  Pro systémy 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 o produktu `@class` naleznete v tématu **setmqaut** .

- Windows

  U systémů Windows zadejte stejné příkazy jako pro systémy AIX and Linux , ale použijte název profilu @CLASS místo @class.

- IBM i

  Pro IBM izadejte tento příkaz:

  ```
  GRTMQMAUT OBJ(*ALL) OBJTYPE(*ALL) USER(' GroupName ') AUT(*ALLADM) MQMNAME(' QMgrName ')
  ```

- z/OS

  Pro 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, ke které má být udělen přístup.

Odebrání konektivity ke správci front

Pokud nechcete, aby se uživatelské aplikace připojovaly k vašemu správci front, odeberte jejich oprávnění pro připojení k tomuto správci front.

Informace o této úloze

Odvolejte oprávnění všech uživatelů pro připojení ke správci front pomocí příslušného příkazu pro váš operační systém.

V systému Multiplatformsmůžete také použít příkaz DELETE AUTHREC .

Poznámka: V produktu 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 IBM izadejte tento příkaz:

  ```
  RVKMQMAUT OBJ ('QMgrName') OBJTYPE(*MQM) USER(*ALL) AUT(*CONNECT)
  ```

- z/OS

  Pro 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)
  ```

  Nevystavujte 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, kterému má být odepřen přístup.

Povolení připojení uživatelských aplikací k vašemu správci front

Chcete povolit uživatelům aplikace připojit se k vašemu správci front. Použijte tabulky uvedené v tomto tématu k určení akcí, které mají být provedeny.

Nejprve určete, zda se klientské aplikace budou připojovat ke správci front.

Pokud žádná z aplikací, které se nebudou připojovat k vašemu správci front, jsou klientské aplikace, zakažte vzdálený přístup, jak je popsáno v tématu “Zakázání vzdáleného přístupu ke správci front” na stránce 380.

Je-li jedna nebo více aplikací, které se připojují ke správci front, klientské aplikace, zajistěte vzdálenou konektivitu podle popisu v části “Zabezpečení vzdáleného připojení ke správci front” na stránce 374.

V obou případech nastavte zabezpečení připojení podle popisu v části “Nastavení zabezpečení připojení” na stránce 381 .

Chcete-li řídit přístup k prostředkům pro každého uživatele připojujícího se ke správci front, prohlédněte si následující tabulku. Je-li příkaz v prvním sloupci true, proveďte akci uvedenou ve druhém sloupci.

Příkaz	**Provést tuto akci**
Máte aplikace, které využívají fronty.	Viz “Řízení uživatelského přístupu k frontám” na stránce 381
Máte aplikace, které využívají témata	Viz “Řízení přístupu uživatelů k tématům” na stránce 387.
Máte aplikace, které se dotazujete na objekt správce front	Viz “Udělení oprávnění k dotazům na správce front” na stránce 388.
Máte aplikace, které používají objekty procesu	Viz “Udělení oprávnění pro přístup k procesům” na stránce 389
Máte aplikace, které používají seznamy názvů	Viz “Udělení oprávnění pro přístup k seznamům názvů” na stránce 390

Zabezpečení vzdáleného připojení ke správci front

Vzdálenou připojitelnost ke správci front můžete zabezpečit pomocí protokolu TLS, ukončení zabezpečení, záznamů ověřování kanálu nebo kombinace těchto metod.

Informace o této úloze

Klienta připojíte ke správci front pomocí kanálu klienta připojení na pracovní stanici klienta a kanálu připojení serveru na serveru. Zabezpečte tato připojení jedním z následujících způsobů.

Postup

1. Použití TLS se záznamy ověření kanálu:
   a) Zabraňte jakémukoliv Distinguished Name (DN) z otevření kanálu tak, že použijete záznam ověření kanálu SSLPEERMAP k mapování všech DN na USERSRC (NOACCESS).
   b) Povolit specifickým jménům DN nebo sad DN pro otevření kanálu pomocí záznamu ověřování kanálu SSLPEERMAP, který je namapuje na USERSRC (CHANNEL).
2. Použití TLS s uživatelskou procedurou zabezpečení:
   a) Nastavte hodnotu MCAUSER na kanálu připojení serveru na identifikátor uživatele bez oprávnění.
   b) Zadejte uživatelskou proceduru zabezpečení pro přiřazení hodnoty MCAUSER v závislosti na hodnotě DN TLS, které obdrží v polích SSLPeerNamePtr a SSLPeerNameLength předaných do uživatelské procedury ve struktuře MQCD.
3. Použití TLS s hodnotami definice pevného kanálu:
   a) Nastavte parametr SSLPEER na kanál připojení serveru na specifickou hodnotu nebo zúžnou škálu hodnot.
   b) Nastavte MCAUSER na kanál připojení serveru na ID uživatele, se kterým má být kanál spuštěn.
4. Použití záznamů ověření kanálu u kanálů, které nepoužívají TLS:
   a) Zabraňte jakýmkoli IP adresám z otevíracích kanálů pomocí záznamu ověřování kanálu mapování adres s parametrem ADDRESS (*) a USERSRC (NOACCESS).
   b) Povolit použití určitých adres IP pro otevírání kanálů pomocí ověřovacích záznamů kanálu mapování adres pro tyto adresy s USERSRC (CHANNEL).
5. Použití uživatelské procedury zabezpečení:
   a) Napište proceduru zabezpečení k autorizaci připojení na základě libovolné vlastnosti, kterou vyberete, například z původní adresy IP.
6. Je také možné použít záznamy ověření kanálu s uživatelskou procedurou pro zabezpečení zprávy nebo použít všechny tři metody, pokud to vaše konkrétní okolnosti vyžadují.

Blokování určitých adres IP

Můžete zabránit tomu, aby specifický kanál přijímal příchozí připojení z adresy IP, nebo zabránil v povolení přístupu z adresy IP pomocí záznamu ověření kanálu.

Než začnete

Povolte záznamy ověření kanálu spuštěním následujícího příkazu:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Informace o této úloze

Chcete-li zakázat přijímání příchozích připojení a ujistit se, že připojení jsou akceptována pouze při použití správného názvu kanálu, lze použít jeden typ pravidla k blokování adres IP. Chcete-li zakázat přístup k adresám IP celému správci front, měli byste za normálních okolností použít ochrannou bariéru (firewall) k trvalému zablokování tohoto správce front. Avšak jiný typ pravidla lze použít k dočasnému zablokování několika adres, například když čekáte na aktualizaci brány firewall.

Procedura

- Chcete-li blokovat adresy IP pomocí specifického kanálu, nastavte záznam ověření 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)
```

K dispozici jsou tři části příkazu:

SET CHLAUTH (*generický-název-kanálu*)
Tuto část příkazu použijete k určení, zda chcete blokovat připojení pro celý 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, který začíná na SYSTEM.
- SET CHLAUTH ('SYSTEM.DEF.SVRCONN')-blokuje kanál SYSTEM.DEF.SVRCONN

Typ pravidla CHLAUTH
Použijte tuto část příkazu k uvedení typu příkazu a určuje, zda chcete zásobovat jednotlivou adresu nebo seznam adres.

Příklad:

- TYPE(ADDRESSMAP) -použijte ADDRESSME, chcete-li zadat jednu adresu nebo zástupný znak. Například ADDRESS('192.168.*') blokuje veškerá spojení přicházející z IP adresy začínající v 192.168.

  Další informace o filtrování adres IP se vzory najdete v tématu Generické adresy IP.
- TYPE(BLOCKADDR) -Použijte BLOCKADDR, pokud chcete dodat seznam adres, které se mají blokovat.

Další parametry
Tyto parametry jsou závislé na typu pravidla, které jste použili ve druhé části příkazu:

- Pro TYPE(ADDRESSMAP) použijte ADDRESS
- Pro TYPE(BLOCKADDR) použijte ADDRLIST

Související odkazy
SET CHLAUTH

Dočasné blokování určitých adres IP v případě, že správce front není spuštěn.
Možná budete chtít blokovat určité adresy IP nebo rozsahy adres, když správce front není spuštěn, a nemůžete proto vydat příkazy MQSC. Můžete dočasně blokovat adresy IP ve výjimečných případech úpravou souboru blockaddr.ini .

Informace o této úloze

Soubor blockaddr.ini obsahuje kopii definic BLOCKADDR, které používá správce front. Tento soubor čte 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 .

Uvědomte si však, že když je správce front spuštěn, zapíše sadu definic BLOCKADDR do souboru blockaddr.ini , přepsáním všech ručních úprav, které jste mohli provést. 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** , je-li správce front spuštěn.

Postup

1. Otevřete soubor blockaddr.ini v textovém editoru.

Soubor je umístěn v datovém adresáři správce front.

2. Přidejte adresy IP jako jednoduché dvojice klíčové slovo-hodnota, kde klíčové slovo je `Addr`.

   Informace o filtrování adres IP se vzory najdete v tématu Generické adresy IP.

   Příklad:

```
Addr = 192.0.2.0
Addr = 192.0.*
Addr = 192.0.2.1-8
```

Související úlohy

“Blokování určitých adres IP” na stránce 374
Můžete zabránit tomu, aby specifický kanál přijímal příchozí připojení z adresy IP, nebo zabránil v povolení přístupu z adresy IP pomocí záznamu ověření kanálu.

Související odkazy

SET CHLAUTH

Blokování specifických ID uživatelů

Určením ID uživatelů můžete zabránit určitým uživatelům v používání kanálu zadáním ID uživatele, pokud je aktivován, aby byl kanál ukončen. To lze provést nastavením záznamu ověřování kanálu.

Než začnete

Ujistěte se, že jsou záznamy ověření kanálu 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)
```

generic-channel-name je název kanálu, ke kterému chcete řídit přístup, nebo vzor obsahující symbol hvězdičky (*) jako zástupný znak, který odpovídá názvu kanálu.

Seznam uživatelů poskytnutý v produktu `TYPE(BLOCKUSER)` se vztahuje pouze na kanály SVRCONN a nikoli na správce front pro kanály správce front.

userID1 a *userID2* jsou ID uživatele, kterému má být bráněno v použití kanálu. Také můžete uvést speciální hodnotu `*MQADMIN` , která se bude odkazovat na privilegované administrativní uživatele. Další informace o privilegovaných uživatelích naleznete v tématu “Oprávnění uživatelé” na stránce 325. Další informace o příkazu `*MQADMIN`naleznete v části SET CHLAUTH.

Související odkazy

SET CHLAUTH

Mapování vzdáleného správce front na ID uživatele MCAUSER

K nastavení atributu MCAUSER kanálu podle správce front, ze kterého se kanál připojuje, můžete použít záznam ověření kanálu.

Než začnete

Ujistěte se, že jsou záznamy ověření kanálu 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. Uvedete-li název kanálu připojení serveru v následujících příkazech, nebude mít žádný účinek.

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)
```

  generic-channel-name je název kanálu, ke kterému chcete řídit přístup, nebo vzor obsahující symbol hvězdičky (*) jako zástupný znak, který odpovídá názvu kanálu.
  generický-partner-qmgr-name je buď název správce front, nebo vzor obsahující symbol hvězdičky (*) jako zástupný znak, který odpovídá názvu správce front.
  uživatel je ID uživatele, které má být použito pro všechna připojení z uvedeného správce front.

- Chcete-li omezit tento příkaz na určité IP adresy, začleňte parametr **ADDRESS** následujícím způsobem:

```
SET CHLAUTH(' generic-channel-name ') TYPE (QMGRMAP) QMNAME(generic-partner-qmgr-name
) USERSRC(MAP) MCAUSER(user) ADDRESS(
generic-ip-address)
```

  generic-channel-name je název kanálu, ke kterému chcete řídit přístup, nebo vzor obsahující symbol hvězdičky (*) jako zástupný znak, který odpovídá názvu kanálu.
  generická-adresa-ip je buď jednotlivá adresa, nebo vzor obsahující symbol hvězdičky (*) jako zástupný znak nebo znak pomlčky (-), který určuje rozsah, který odpovídá adrese. Další informace o generických adresách IP najdete v tématu Generické IP adresy.

Související odkazy
SET CHLAUTH

Mapování ID uživatele klienta na ID uživatele MCAUSER
Záznam ověření kanálu můžete použít ke změně atributu MCAUSER kanálu připojení serveru podle ID uživatele přijatého od klienta.

Než začnete

Ujistěte se, že jsou záznamy ověření kanálu 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 ostatní typy kanálů.

Postup

Nastavte záznam ověřování kanálu pomocí příkazu MQSC **SET CHLAUTH**nebo příkazu PCF příkazu **Set Channel Authentication Record** . Můžete například zadat příkaz MQSC:

```
SET CHLAUTH(' generic-channel-name ') TYPE (USERMAP) CLNTUSER(client-user-name) USERSRC(MAP)
MCAUSER(
user)
```

generic-channel-name je název kanálu, ke kterému chcete řídit přístup, nebo vzor obsahující symbol hvězdičky (*) jako zástupný znak, který odpovídá názvu kanálu.

client-user-name je ID uživatele přidružené k připojení klientů, hodnota může být deklarována klientskou aplikací, změněna pomocí ověření připojení pomocí předčasného přijetí nebo nastavení prostřednictvím uživatelské procedury kanálu.

user je ID uživatele, které má být použito místo jména uživatele klienta.

Související odkazy

SET CHLAUTH

Atributy stanzy channels (ChlauthEarlyAdopt)

Mapování rozlišovacího jména SSL nebo TLS na ID uživatele MCAUSER

Můžete použít záznam ověření kanálu k nastavení atributu MCAUSER kanálu, podle přijatého rozlišovacího názvu (DN).

Než začnete

Ujistěte se, že jsou záznamy ověření kanálu 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)
```

generic-channel-name je 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 následující za standardními pravidly IBM MQ pro hodnoty SSLPEER. Viz IBM MQ pravidla pro hodnoty SSLPEER.

uživatel je ID uživatele, které má být použito pro všechna připojení používající zadané DN.

generický-vydavatel-název odkazuje na DN vydávajícího certifikátu, který má odpovídat. Tento parametr je volitelný, ale měli byste jej použít, abyste se vyhnuli chybnému porovnávání chybného certifikátu, pokud se používá více certifikačních autorit.

Související odkazy

SET CHLAUTH

Blokování přístupu ze vzdáleného správce front

Záznam ověření kanálu můžete použít, chcete-li vzdálenému správci front zabránit v spouštění kanálů.

Než začnete

Ujistěte se, že jsou záznamy ověření kanálu povoleny následujícím způsobem:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Informace o této úloze

Všimněte si, že tato technika se nevztahuje na kanály připojení serveru. Zadáte-li v následujícím příkazu název kanálu připojení serveru, nebude mít žádný účinek.

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)
```

generic-channel-name je název kanálu, ke kterému chcete řídit přístup, nebo vzor obsahující symbol hvězdičky (*) jako zástupný znak, který odpovídá názvu kanálu.

generický-partner-qmgr-name je buď název správce front, nebo vzor obsahující symbol hvězdičky (*) jako zástupný znak, který odpovídá názvu správce front.

Související odkazy

SET CHLAUTH

Blokování přístupu pro ID uživatele klienta

Záznam ověření kanálu můžete použít, chcete-li zabránit ID uživatele klienta při vytváření připojení kanálu.

Než začnete

Ujistěte se, že jsou záznamy ověření kanálu 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 ostatní 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)
```

generic-channel-name je název kanálu, ke kterému chcete řídit přístup, nebo vzor obsahující symbol hvězdičky (*) jako zástupný znak, který odpovídá názvu kanálu.

client-user-name je ID uživatele přidružené k připojení klientů, hodnota může být deklarována klientskou aplikací, změněna pomocí ověření připojení pomocí předčasného přijetí nebo nastavení prostřednictvím uživatelské procedury kanálu.

Související odkazy

SET CHLAUTH

Blokování přístupu pro rozlišující název SSL nebo TLS

Záznam ověření kanálu můžete použít k zabránění rozlišujícího názvu (DN) TLS ze spuštění kanálů.

Než začnete

Ujistěte se, že jsou záznamy ověření kanálu 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)
```

generic-channel-name je 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 následující za standardními pravidly IBM MQ pro hodnoty SSLPEER. Viz IBM MQ pravidla pro hodnoty SSLPEER.

generický-vydavatel-název odkazuje na DN vydávajícího certifikátu, který má odpovídat. Tento parametr je volitelný, ale měli byste jej použít, abyste se vyhnuli chybnému porovnávání chybného certifikátu, pokud se používá více certifikačních autorit.

Související odkazy

SET CHLAUTH

Mapování adresy IP na ID uživatele MCAUSER

Můžete použít záznam ověření kanálu k nastavení atributu MCAUSER kanálu, podle IP adresy, ze které je připojení přijato.

Než začnete

Ujistěte se, že jsou záznamy ověření kanálu 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)
```

generic-channel-name je název kanálu, ke kterému chcete řídit přístup, nebo vzor obsahující symbol hvězdičky (*) jako zástupný znak, který odpovídá názvu kanálu.

uživatel je ID uživatele, které má být použito pro všechna připojení používající zadané DN.

generická-ip-adresa je buď adresa, ze které se vytváří připojení, nebo vzor obsahující hvězdičku (*) jako zástupný znak nebo pomlčku (-) pro označení rozsahu, který odpovídá adrese.

Související odkazy

SET CHLAUTH

Zakázání vzdáleného přístupu ke správci front

Pokud nechcete, aby se klientské aplikace připojovaly ke svému správci front, zakažte vzdálený přístup k této aplikaci.

Informace o této úloze

Zabraňte klientským aplikacím, které se připojují ke správci front jedním z následujících způsobů:

Procedura

- Odstraňte všechny kanály připojení serveru pomocí příkazu MQSC **DELETE CHANNEL**.

- Nastavte identifikátor uživatele kanálu zpráv (MCAUSER) kanálu na ID uživatele bez přístupových práv pomocí příkazu MQSC **ALTER CHANNEL**.

Nastavení zabezpečení připojení

Udělte oprávnění pro připojení ke správci front každému uživateli nebo skupině uživatelů, kteří mají obchodní potřebu, aby tak mohli učinit.

Informace o této úloze

Chcete-li nastavit zabezpečení připojení, použijte příslušné příkazy pro váš operační systém.

Na platformách pro více platforem můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance lze 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 pro připojení k dávce, CICS, IMS a inicializátoru kanálu (CHIN). Pokud nepoužíváte 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 generický profil, pro které chcete změnit autorizace.

  GroupName
  Název skupiny, ke které má být udělen přístup.

Související pojmy

“Profily zabezpečení připojení pro inicializátor kanálu” na stránce 193
Profily pro kontrolu připojení z inicializátoru kanálu se skládají ze správce front nebo názvu skupiny sdílení front následovaného slovem *CHIN*. Zadejte ID uživatele použité inicializatorem kanálu s přístupem k profilu připojení READ k profilu připojení.

Řízení uživatelského přístupu k frontám

Chcete řídit přístup aplikací k frontám. Použijte toto téma k určení, jaké akce se mají provést.

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 382
Kontext sady aplikací	Viz “Udělení oprávnění pro nastavení kontextu” na stránce 383
Aplikace předává kontext	Viz “Udělení oprávnění pro předání kontextu” na stránce 384
Aplikace ukládá zprávy do klastrované fronty.	Viz “Autorizace vkládání zpráv ve vzdálených frontách klastru” na stránce 467
Aplikace vkládá zprávy do lokální fronty	Viz “Udělení oprávnění k vkládání zpráv do lokální fronty” na stránce 384
Aplikace vkládá zprávy do modelové fronty	Viz “Udělení oprávnění k vkládání zpráv do modelové fronty” na stránce 385
Aplikace vkládá zprávy do vzdálené fronty	Viz “Udělení oprávnění pro vkládání zpráv do vzdálené fronty klastru” na stránce 386

Udělení oprávnění k získání zpráv z front
Udělte oprávnění pro získání zpráv z fronty nebo sady front pro každou skupinu uživatelů, kteří pro ni potřebují obchodní potřeby.

Informace o této úloze

Chcete-li udělit oprávnění k získání zpráv z některých front, použijte příslušné příkazy pro váš operační systém.

Na platformách pro více platforem můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance lze 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 IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*GET) MQMNAME(' QMgrName ')
```

- Pro 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 generický profil, pro které chcete změnit autorizace.

GroupName
Název skupiny, ke které má být udělen přístup.

Udělení oprávnění pro nastavení kontextu
Udělte oprávnění pro nastavení kontextu na zprávu, která je vložena, pro každou skupinu uživatelů, kteří pro ni potřebují obchodní potřeby.

Informace o této úloze

Chcete-li udělit oprávnění pro nastavení kontextu v některých frontách, použijte příslušné příkazy pro daný operační systém.

Na platformách pro více platforem můžete také použít příkaz SET AUTHREC .

Poznámka: 

V systému IBM MQ Appliance lze použít pouze příkaz **SET AUTHREC** .

Procedura

- U systémů AIX, Linux, and Windows zadejte jeden z následujících příkazů:
  - Chcete-li nastavit pouze kontext identity:

    ```
    setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +setid
    ```

  - Chcete-li nastavit celý kontext:

    ```
    setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +setall
    ```

  Poznámka: Chcete-li použít oprávnění `setid` nebo `setall` , autorizace musí být udělena jak pro příslušný objekt fronty, tak i pro objekt správce front.
- Pro IBM izadejte jeden z následujících příkazů:
  - Chcete-li nastavit pouze kontext identity:

    ```
    GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*SETID) MQMNAME('
    QMgrName ')
    ```

  - Chcete-li nastavit celý kontext:

    ```
    GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*SETALL) MQMNAME('
    QMgrName ')
    ```

- Pro z/OSzadejte jednu z následujících sad příkazů:
  - Chcete-li nastavit pouze kontext identity:

    ```
    RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
    PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
    ```

  - Chcete-li nastavit celý kontext:

    ```
    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 generický profil, pro které chcete změnit autorizace.

  GroupName
  Název skupiny, ke které má být udělen přístup.

Udělení oprávnění pro předání kontextu
Udělte oprávnění pro předávání kontextu z načtené zprávy do každé skupiny uživatelů, kteří pro ni mají obchodní potřebu.

Informace o této úloze

Chcete-li udělit oprávnění pro předávání kontextu v některých frontách, použijte příslušné příkazy pro daný operační systém.

Na platformách pro více platforem můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance lze použít pouze příkaz **SET AUTHREC** .

Procedura

- ALW

  U systémů AIX, Linux, and Windows zadejte jeden z následujících příkazů:

  - Chcete-li předat kontext identity pouze:

    ```
    setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +passid
    ```

  - Chcete-li předat celý kontext:

    ```
    setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +passall
    ```

- IBM i

  Pro IBM izadejte jeden z následujících příkazů:

  - Chcete-li předat kontext identity pouze:

    ```
    GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*PASSID) MQMNAME('
    QMgrName ')
    ```

  - Chcete-li předat celý kontext:

    ```
    GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*PASSALL) MQMNAME('
    QMgrName ')
    ```

- z/OS

  Chcete-li předat kontext identity nebo celý kontext, zadejte pro příkaz z/OSnásledující 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 generický profil, pro které chcete změnit autorizace.

  GroupName
  Název skupiny, ke které má být udělen přístup.

Udělení oprávnění k vkládání zpráv do lokální fronty
Udělte oprávnění pro vkládání zpráv do lokální fronty nebo sady front do každé skupiny uživatelů, kteří pro ni potřebují obchodní potřeby.

Informace o této úloze

Chcete-li udělit oprávnění pro vkládání zpráv do některých lokálních front, použijte příslušné příkazy pro daný operační systém.

Na platformách pro více platforem můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance lze 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 IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*PUT) MQMNAME(' QMgrName ')
```

- Pro 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 generický profil, pro které chcete změnit autorizace.

  GroupName
  Název skupiny, ke které má být udělen přístup.

Udělení oprávnění k vkládání zpráv do modelové fronty
Udělte oprávnění pro vkládání zpráv do modelové fronty nebo sady modelových front pro každou skupinu uživatelů, kteří pro ni potřebují obchodní potřeby.

Informace o této úloze

Modelové fronty se používají k vytváření dynamických front. Musíte proto udělit oprávnění pro model i pro dynamické fronty. Chcete-li tyto oprávnění udělit, použijte příslušné příkazy pro váš operační systém.

Na platformách pro více platforem můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance lze použít pouze příkaz **SET AUTHREC** .

Procedura

- Pro systémy 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 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 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 generický profil, pro které se mají změnit autorizace.

GroupName
Název skupiny, ke které má být udělen přístup.

Udělení oprávnění pro vkládání zpráv do vzdálené fronty klastru
Udělte oprávnění pro vkládání zpráv do vzdálené fronty klastru nebo do fronty, do každé skupiny uživatelů, kteří pro ni potřebují obchodní potřeby.

Informace o této úloze

Chcete-li vložit zprávu do fronty vzdáleného klastru, můžete ji buď umístit na lokální definici vzdálené fronty, nebo zcela kvalifikovanou vzdálenou frontu. Používáte-li lokální definici vzdálené fronty, potřebujete oprávnění k umístění lokálního objektu: viz “Udělení oprávnění k vkládání zpráv do lokální fronty” na stránce 384. Používáte-li plně kvalifikovanou vzdálenou frontu, musíte mít oprávnění k umístění 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 konfigurovali atribut **ClusterQueueAccessControl** v souboru qm.ini na hodnotu *RQMName*, jak je popsáno v tématu Sekce zabezpečení , a restartováním správce front.

Na platformách pro více platforem můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance lze 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 můžete použít objekt *rqmname* pouze pro vzdálené fronty klastru.

- Pro IBM izadejte tento příkaz:

```
GRTMQMAUT OBJTYPE(*RMTMQMNAME) OBJ('
ObjectProfile') USER(GroupName) AUT(*PUT) MQMNAME('
QMgrName')
```

Všimněte si, že můžete použít objekt RMTMQMNAME pouze pro vzdálené fronty klastru.

- Pro z/OSzadejte následující příkazy:

```
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
```

```
PERMIT QMgrName.QUEUE.ObjectProfile CLASS(MQQUEUE)
ID(GroupName) ACCESS(UPDATE)
```

Všimněte si, že můžete použít název vzdáleného správce front (nebo skupiny sdílení front) pouze pro vzdálené fronty 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 generický profil, pro které chcete změnit autorizace.

GroupName
Název skupiny, ke které má být udělen přístup.

Řízení přístupu uživatelů k tématům

Je třeba řídit přístup aplikací k tématům. Použijte toto téma k určení, jaké akce se mají provést.

Pro každý pravdivý příkaz v prvním sloupci proveďte akci uvedenou ve druhém sloupci.

Tabulka 71. Řízení přístupu uživatelů k tématům

Příkaz	**Akce**
Aplikace publikuje zprávy do tématu	Viz “Udělení oprávnění pro publikování zpráv do tématu” na stránce 387
Aplikace se přihlásí k odběru tématu.	Viz “Udělení oprávnění k odběru témat” na stránce 388

Udělení oprávnění pro publikování zpráv do tématu

Udělte oprávnění pro publikování zpráv na téma nebo sadu témat, pro každou skupinu uživatelů, kteří pro ni potřebují obchodní potřeby.

Informace o této úloze

Chcete-li udělit oprávnění k publikování zpráv do některých témat, použijte příslušné příkazy pro váš operační systém.

Na platformách pro více platforem můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance lze 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 IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*TOPIC) USER(GroupName) AUT(*PUB) MQMNAME('
QMgrName ')
```

- Pro 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 generický profil, pro které chcete změnit autorizace.

GroupName
Název skupiny, ke které má být udělen přístup.

Udělení oprávnění k odběru témat
Udělte oprávnění k odběru tématu nebo sady témat pro každou skupinu uživatelů, kteří pro ni mají obchodní potřebu.

Informace o této úloze

Chcete-li udělit oprávnění přihlásit se k odběru některých témat, použijte příslušné příkazy pro váš operační systém.

Na platformách pro více platforem můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance lze 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 IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*TOPIC) USER(GroupName) AUT(*SUB) MQMNAME('
QMgrName ')
```

- Pro 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 generický profil, pro které chcete změnit autorizace.

GroupName
Název skupiny, ke které má být udělen přístup.

Udělení oprávnění k dotazům na správce front

Udělte oprávnění k dotazům na správce front, do každé skupiny uživatelů, kteří pro ni potřebují obchodní potřeby.

Informace o této úloze

Chcete-li udělit oprávnění k dotazům na správce front, použijte příslušné příkazy pro váš operační systém.

Na platformách pro více platforem můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance lze 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 IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*MQM) USER(GroupName) AUT(*INQ) MQMNAME(' QMgrName
')
```

- Pro z/OSzadejte následující příkazy:

```
RDEFINE MQCMDS QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

  Tyto příkazy udělují přístup k uvedenému 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 generický profil, pro které chcete změnit autorizace.

  GroupName
  Název skupiny, ke které má být udělen přístup.

Udělení oprávnění pro přístup k procesům

Udělte oprávnění pro přístup k procesu nebo sadě procesů, pro každou skupinu uživatelů, kteří pro ni potřebují obchodní potřeby.

Informace o této úloze

Chcete-li udělit oprávnění pro přístup k některým procesům, použijte příslušné příkazy pro váš operační systém.

Na platformách pro více platforem můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance lze 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 IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*PRC) USER(GroupName) AUT(*ALL) MQMNAME(' QMgrName
')
```

- Pro 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 generický profil, pro které chcete změnit autorizace.

GroupName
Název skupiny, ke které má být udělen přístup.

Udělení oprávnění pro přístup k seznamům názvů

Udělte oprávnění pro přístup k seznamu názvů nebo sadě seznamů názvů, pro každou skupinu uživatelů, kteří pro ni potřebují obchodní položku.

Informace o této úloze

Chcete-li udělit oprávnění pro přístup k některým seznamům názvů, použijte příslušné příkazy pro váš operační systém.

Na platformách pro více platforem můžete také použít příkaz SET AUTHREC .

Poznámka: MQ Appliance V systému IBM MQ Appliance lze 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 IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ('ObjectProfile
') OBJTYPE(*NMLIST) USER(GroupName) AUT(*ALL) MQMNAME('
QMgrName')
```

- Pro 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 generický profil, pro které chcete změnit autorizace.

GroupName
Název skupiny, ke které má být udělen přístup.

ALW Oprávnění ke správě produktu IBM MQ v systému AIX, Linux, and Windows

Administrátoři produktu IBM MQ mohou používat všechny příkazy produktu IBM MQ a udělovat oprávnění ostatním uživatelům. Když administrátoři vydají příkazy vzdáleným správcům front, musí mít požadované oprávnění ve vzdáleném správci front. Další pokyny platí pro systémy Windows .

Administrátoři produktu IBM MQ mají oprávnění k používání všech příkazů produktu IBM MQ (včetně příkazů pro udělení oprávnění IBM MQ pro jiné uživatele).

Chcete-li být administrátorem produktu IBM MQ , musíte být členem speciální skupiny, která se nazývá skupina **mqm** .

Windows Případně pouze v systému Windows může lokální účty spravovat IBM MQ , pokud jsou členy skupiny Administrators na systémech Windows .

Upozornění: Uživatele produktu Azure AD můžete do skupiny mqm přidat pomocí příkazu administrátora. Použijte například příkaz `net localgroup mqm AzureAD\<your userID> /add`. Poté spusťte příkazy administrace produktu IBM MQ nebo použijte příkaz IBM MQ Explorer.

Skupina **mqm** se vytvoří automaticky při instalaci produktu IBM MQ . Do skupiny můžete přidávat další uživatele, které 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 používat řídicí příkazy ke správě produktu IBM MQ. Jeden z těchto řídicích příkazů je **setmqaut**, který se používá k udělení oprávnění jiným uživatelům, aby jim bylo umožněno přistupovat k prostředkům IBM MQ nebo řídit jejich řízení. Příkazy PCF pro správu záznamů oprávnění jsou dostupné pro neadministrátory, kteří jsou správci front udělovali dsp a chg oprávnění. Další informace o správě oprávnění pomocí příkazů PCF najdete v tématu Programovatelné formáty příkazů.

Administrátoři musí mít požadovaná oprávnění pro příkazy MQSC, které mají být zpracovány vzdáleným správcem front. Produkt IBM MQ Explorer vydává příkazy PCF pro provádění administrativních úloh. Administrátoři nepotřebují další oprávnění k používání produktu IBM MQ Explorer k administraci správce front v lokálním systému. Je-li produkt IBM MQ Explorer použit ke správě správce front v jiném systému, musí mít administrátoři oprávnění pro příkazy PCF, které má zpracovat vzdálený správce front.

Upozornění: Z produktu IBM MQ 8.0nemusíte být administrátorem, abyste mohli použít řídicí příkaz **runmqsc**, který vydává příkazy skriptu IBM MQ Script (MQSC).

Je-li produkt **runmqsc** použit v nepřímém režimu k odeslání příkazů MQSC do vzdáleného správce front, je každý příkaz MQSC zapouzdřen v rámci příkazu Escape PCF.

Další informace o kontrolách oprávnění, jsou-li zpracovány příkazy PCF a MQSC, najdete v následujících tématech:

- Pro příkazy PCF, které pracují se správci front, frontami, procesy, seznamy názvů a objekty ověřovacích informací, viz Oprávnění pro práci s objekty IBM MQ. Informace o ekvivalentních příkazech MQSC zapouzdřených v příkazech Escape PCF najdete v této sekci.
- Pro příkazy PCF, které pracují s kanály, inicializátory kanálu, listenery a klastry, naleznete informace v tématu Zabezpečení kanálů.
- Pro příkazy PCF, které pracují se záznamy oprávnění, viz Kontrola oprávnění pro příkazy PCF
- z/OS U příkazů MQSC, které jsou zpracovány příkazovým serverem v systému IBM MQ for z/OS, naleznete informace v tématu Zabezpečení příkazů a zabezpečení prostředků příkazů v systému z/OS .

Kromě toho má účet SYSTEM v systémech Windows úplný přístup k prostředkům produktu IBM MQ .

Na platformách AIX and Linux je rovněž vytvořeno speciální ID uživatele produktu **mqm** , které bude používat pouze produkt. Nesmí být nikdy k dispozici pro neprivilegované uživatele. Všechny objekty produktu IBM MQ jsou vlastněny ID uživatele **mqm**.

V systémech Windows mohou členové skupiny administrátorů také spravovat libovolného správce front, jako je například účet SYSTEM. Můžete také vytvořit skupinu domén **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 u objektů IBM MQ a potřebují oprávnění pro práci s těmito objekty (jak je popsáno v následujících oddílech). Členové skupiny **mqm** mají oprávnění pracovat se všemi objekty, ale v systémech Windows mohou nastat okolnosti, pokud je oprávnění odepřeno, pokud máte lokálního uživatele a uživatele s ověřenou doménou se stejným názvem. Tento popis je popsán v tématu “Činitelé a skupiny v systému AIX, Linux, and Windows” na stránce 395.

Windows verzí s funkcí UAC (User Account Control) omezuje akce, které mohou uživatelé provádět na určitých zařízeních operačního systému, i když jsou členy skupiny Administrators. Pokud je vaše ID uživatele ve skupině administrátorů, ale ne ve skupině **mqm** , musíte použít zvýšený příkazový řádek k vydání příkazů administrátora produktu IBM MQ , jako je **crtmqm**, v opačném případě je vygenerována 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 na ikonu na příkazový řádek a vyberte volbu **Spustit jako administrátor**.

Chcete-li provést následující akce, nemusíte být členem skupiny **mqm** :

- Vydejte příkazy z aplikačního programu, který vydává příkazy PCF, nebo příkazy MQSC v příkazu Escape PCF, pokud příkazy manipulují inicializátory kanálu. (Tyto příkazy jsou popsány v části “Zabezpečení definic inicializátoru kanálu” na stránce 109).
- Vydejte volání MQI z aplikačního programu (pokud nechcete použít vazby rychlé cesty na volání `MQCONNX`).
- Použijte příkaz `crtmqcvx` k vytvoření fragmentu kódu, který provádí převod dat na strukturách datových typů.
- Použijte příkaz `dspmq` k zobrazení správců front.
- Pomocí příkazu `dspmqtrc` zobrazte formátovaný výstup trasování obslužného programu IBM MQ .

Omezení 12 znaků se týká jak skupin, tak ID uživatelů.

Platformy UNIX and Linux obecně omezují délku ID uživatele na 12 znaků. AIX 5.3 tento limit zvýšil, ale produkt IBM MQ pokračuje ve sledování omezení 12 znaků na všech platformách UNIX and Linux . Použijete-li ID uživatele větší než 12 znaků, nahradí jej produkt IBM MQ hodnotou `UNKNOWN`. Nedefinujte ID uživatele s hodnotou `UNKNOWN`.

ALW Správa skupiny mqm v systému AIX, Linux, and Windows

Uživatelům v skupině mqm jsou udělena úplná administrativní oprávnění k produktu IBM MQ. Z tohoto důvodu byste neměli zapisovat aplikace a běžné uživatele do skupiny mqm. Skupina mqm by měla obsahovat pouze účty administrátorů produktu IBM MQ .

Tyto úlohy jsou popsány v následujících tématech:

- Windows Vytvoření a správa skupin v systému Windows
- AIX Vytvoření a správa skupin v systému AIX
- Linux Vytvoření a správa skupin v systému Linux

Windows Pokud váš řadič domény běží v systému Windows 2000 nebo Windows 2003 nebo později, může administrátor vaší domény nastavit speciální účet, který má produkt IBM MQ používat. Další informace viz Konfigurace IBM MQ s Prepare IBM MQ Wizard a Vytvoření a nastavení Windows účtů domény pro IBM MQ.

ALW Oprávnění pro práci s objekty IBM MQ v systému AIX, Linux, and Windows

Všechny objekty jsou chráněny produktem IBM MQa činitelé musí mít odpovídající oprávnění pro přístup k nim. Různí činitelé potřebují různá přístupová práva k různým objektům.

Správci front, fronty, definice procesů, seznamy názvů, kanály, kanály připojení klienta, moduly listener, služby a objekty ověřovacích informací jsou všechny přístupné z aplikací, které používají volání MQI nebo příkazy PCF. Tyto prostředky jsou všechny chráněny produktem IBM MQa aplikace musí mít oprávnění k přístupu k nim. Entita, která vydává požadavek, může být uživatel, aplikační program, který vydává volání MQI, nebo administrativní program, který vydává příkaz PCF. Identifikátor žadatele je označován jako *činitel*.

Různým skupinám činitelů lze udělit různé typy přístupových oprávnění ke stejnému objektu. Například u určité fronty může být jedna skupina povolena k provádění operací put a get. Jiná skupina může být povolena pouze k procházení fronty (MQGET s volbou procházení). Podobně některé skupiny mohou mít k frontě oprávnění k vložení a získání oprávnění ke frontě, ale nesmí jim být dovoleno měnit atributy fronty nebo je odstraňovat.

Některé operace jsou zvláště 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
- Vytváření a odstraňování front aplikací

Oprávnění k úplnému přístupu k objektu je automaticky přiděleno ID uživatele, který objekt vytvořil, a všem členům skupiny mqm (a členům lokální skupiny administrátorů v systému Windows).

Související pojmy

“Oprávnění ke správě produktu IBM MQ v systému AIX, Linux, and Windows” na stránce 391
Administrátoři produktu IBM MQ mohou používat všechny příkazy produktu IBM MQ a udělovat oprávnění ostatním uživatelům. Když administrátoři vydají příkazy vzdáleným správcům front, musí mít požadované oprávnění ve vzdáleném správci front. Další pokyny platí pro systémy Windows .

ALW Když jsou provedeny kontroly zabezpečení na AIX, Linux, and Windows

Kontroly zabezpečení jsou obvykle prováděny při připojování ke správci front, při otevírání nebo zavírání objektů a při vkládání nebo načítání zpráv.

Kontroly zabezpečení provedené pro typickou aplikaci jsou následující:

Připojování ke správci front (volání MQCONN nebo MQCONNX)
Toto je poprvé, kdy je aplikace asociována s konkrétním správcem front. Správce front dotazuje operační prostředí ke zjištění ID uživatele přidruženého k aplikaci. Produkt IBM MQ potom ověřuje, zda je ID uživatele autorizováno pro připojení ke správci front, a zachová ID uživatele pro budoucí kontroly.

Uživatelé se nemusí přihlašovat k produktu IBM MQ; produkt IBM MQ předpokládá, že uživatelé se přihlásili k základnímu operačnímu systému a byli ověřeni tímto způsobem.

Otevření objektu (volání MQOPEN nebo MQPUT1)
K objektům produktu IBM MQ se přistupuje otevřením objektu a zadáním jeho příkazů. Všechny kontroly prostředků se provádějí při otevření objektu, spíše než při jejich skutečnému přístupu. To znamená, že požadavek **MQOPEN** musí uvádět požadovaný typ přístupu (například to, zda uživatel chce pouze procházet objekt nebo provést aktualizaci jako vkládání zpráv do fronty).

Produkt IBM MQ zkontroluje prostředek, který je uveden v požadavku **MQOPEN** . Pro alias nebo objekt vzdálené fronty je použitá autorizace sama o sobě pro objekt, nikoli frontu, na kterou je rozlišen alias nebo vzdálená fronta. To znamená, že uživatel nepotřebuje oprávnění pro přístup k němu. Omezte oprávnění k vytváření front pro privilegované uživatele. Pokud tomu tak není, uživatelé mohou obejít

normální řízení přístupu pouhým vytvořením aliasu. Je-li vzdálená fronta odkazována explicitně spolu s názvy fronty i správce front, je zkontrolována přenosová fronta přidružená ke vzdálenému správci front.

Oprávnění k dynamické frontě je založeno na tom, které z modelové fronty je odvozeno, ale nemusí být nutně stejné. Tento popis je popsán v poznámce “1” na stránce 128.

ID uživatele použité správcem front pro kontroly přístupu je ID uživatele získaného z provozního prostředí aplikace připojené ke správci front. Aplikace s vhodnou autorizací může vydat volání **MQOPEN** s uvedením alternativního ID uživatele; kontroly řízení přístupu se pak provedou na alternativním ID uživatele. To nemění ID uživatele přidružené k aplikaci, pouze ta, která se používá pro kontroly řízení přístupu.

Vložení a získání zpráv (volání MQPUT nebo MQGET)
Neprovedou se žádné kontroly řízení přístupu.

Zavření objektu (MQCLOSE)
Nejsou provedeny žádné kontroly řízení přístupu, pokud **MQCLOSE** nezpůsobuje odstranění dynamické fronty. V takovém případě je zde kontrola, že ID uživatele je oprávněno k odstranění fronty.

Přihlášení k odběru tématu (MQSUB)
Když se aplikace přihlašuje k odběru tématu, určuje typ operace, kterou je třeba provést. Jedná se o vytvoření nového odběru, změnu existujícího odběru nebo obnovení existujícího odběru, aniž by došlo k jeho změně. Pro každý typ operace správce front ověří, zda má ID uživatele přidružené k aplikaci oprávnění k provedení operace.

Když se aplikace přihlásí k odběru tématu, provede se kontrola oprávnění k objektům tématu, které se nacházejí ve stromu témat ve stromu témat, v němž je aplikace odebíraná, nebo nad ním. Kontroly oprávnění mohou zahrnovat kontroly více než jednoho objektu tématu.

ID uživatele, které správce front používá pro kontrolu oprávnění, je ID uživatele získané z operačního systému, když se aplikace připojuje ke správci front.

Správce front provádí kontroly oprávnění ve frontách odběratele, ale ne ve spravovaných frontách.

ALW Jak řízení přístupu je implementováno produktem IBM MQ v systému AIX, Linux, and Windows

Produkt IBM MQ používá služby zabezpečení poskytované podkladovým operačním systémem pomocí správce oprávnění k objektu. IBM MQ poskytuje příkazy pro vytváření a údržbu seznamů přístupových práv.

Součástí produktu IBM MQje rozhraní řízení přístupu, které se nazývá rozhraní služeb autorizace. Produkt IBM MQ poskytuje implementaci správce řízení přístupu (vyhovujícího rozhraní autorizační služby) označovaným jako *správce oprávnění k objektu (OAM)*. Toto je automaticky nainstalováno a povoleno pro každého správce front, kterého jste vytvořili, pokud neurčíte jinak (jak je popsáno v “Zabránění kontrolám zabezpečených přístupů na systémech AIX, Linux, and Windows” na stránce 353). OAM může být nahrazen libovolným uživatelem nebo dodavatelem zapsanou komponentou, která je v souladu s rozhraním autorizační služby.

OAM využívá funkce zabezpečení základního operačního systému s použitím ID uživatelů a skupin operačního systému. Uživatelé mohou přistupovat k objektům produktu IBM MQ pouze v případě, že mají správné oprávnění. “Řízení přístupu k objektům pomocí OAM v systému AIX, Linux, and Windows” na stránce 343 popisuje, jak tento úřad udělit a odvolat.

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 Windowsuživatelům ve skupině administrátorů a uživatelé se přihlásili s ID SYSTEM. Uživatelský přístup ke frontě nelze změnit.

IBM MQ poskytuje příkazy pro vytváření a údržbu seznamů přístupových práv. Další informace o těchto příkazech najdete v tématu “Řízení přístupu k objektům pomocí OAM v systému AIX, Linux, and Windows” na stránce 343.

Produkt IBM MQ předává požadavek OAM požadavek obsahující činitel, název prostředku a typ přístupu. OAM uděluje nebo odmítá přístup na základě seznamu ACL, který spravuje. IBM MQ dodržuje rozhodnutí OAM; pokud OAM nemůže učinit rozhodnutí, IBM MQ neumožňuje přístup.

ALW Identifikace ID uživatele v systému AIX, Linux, and Windows

Správce oprávnění k objektu identifikuje činitele, který žádá o přístup k prostředku. ID uživatele použité jako činitel se liší v závislosti na kontextu.

Správce oprávnění k objektu (OAM) musí být schopen identifikovat, kdo žádá o přístup k určitému prostředku. IBM MQ používá termín *činitel* k odkazování na tento identifikátor. Činitel je vytvořen při prvním připojení aplikace ke správci front; je určen správcem front z ID uživatele přidruženého k připojované aplikaci. (Pokud aplikace odesílá volání XA bez připojení ke správci front, bude ID uživatele přidružené k aplikaci, které vydává volání xa_open, použito pro kontrolu oprávnění správce front.)

V systémech AIX and Linux autorizační rutiny kontrolují buď skutečné ID uživatele (logged-in), nebo efektivní ID uživatele přidružené k aplikaci. Zaškrtnuté ID uživatele může záviset na typu vazby, aby se zobrazily podrobnosti v části Instalovatelné služby.

IBM MQ šíří ID uživatele přijaté ze systému v záhlaví zprávy (struktura MQMD) pro každou zprávu 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 398. Aplikace nemohou tyto informace měnit, pokud nemají autorizaci ke změně informací o kontextu.

ALW *Činitelé a skupiny v systému AIX, Linux, and Windows*

Řídicí služby mohou náležet do skupin. Tím, že udělíte přístup k prostředkům spíše skupinám než jednotlivcům, můžete snížit požadované množství administrace. Seznamy přístupových práv (ACL) jsou založeny na skupinách i ID uživatelů.

Můžete například definovat skupinu skládající se z uživatelů, kteří chtějí spustit určitou aplikaci. Ostatní uživatelé mohou mít 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 v systému AIX
- Linux Vytvoření a správa skupin v systému Linux
- Windows Vytvoření a správa skupin v systému Windows

Činitel může náležet do více než jedné skupiny (sada skupin). Má souhrn všech oprávnění udělených každé skupině v rámci své skupiny. Tato oprávnění jsou uložena do mezipaměti, takže všechny změny, které provedete v členství ve skupině, nebudou rozpoznány, dokud nebude správce front restartován, pokud nezadáte příkaz MQSC **REFRESH SECURITY** (nebo ekvivalent jeho PCF).

Linux AIX Systémy AIX and Linux

V produktu IBM MQ 8.0jsou seznamy přístupových práv (ACL) založeny na identifikátorech uživatelů a skupinách a lze je použít buď pro autorizaci nastavením atributu **SecurityPolicy** na příslušnou hodnotu, jak je popsáno v tématu Sekce Service souboru qm.ini a Konfigurace stanzy autorizační služby v systému AIX and Linux.

V produktu IBM MQ 8.0můžete pro autorizaci použít *model založený na uživateli* a můžete použít jak uživatele, tak skupiny. Když však uvedete uživatele v příkazu setmqaut , nová oprávnění se vztahují pouze na tohoto uživatele a ne na skupiny, do kterých tento uživatel patří. Další informace naleznete v tématu Oprávnění založená na uživateli OAM v systémech UNIX a Linux.

Použijete-li pro autorizaci *model založený na skupině* , bude do seznamu přístupových práv zahrnuta primární skupina, do níž patří toto ID uživatele. Individuální ID uživatele není zahrnuto a oprávnění je uděleno všem členům této skupiny. Vzhledem k tomu si buďte vědomi toho, že můžete nechtěně změnit oprávnění činitele změnou oprávnění jiného činitele ve stejné skupině.

Všichni uživatelé jsou přiřazeni k výchozí skupině uživatelů nobody a ve výchozím nastavení nejsou této skupině udělena žádná autorizace. Autorizaci ve skupině nobody můžete změnit, chcete-li uživatelům bez specifických autorizací udělit přístup k prostředkům produktu IBM MQ .

V 9.2.1 Od IBM MQ 9.2.1můžete 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 libovolné ID uživatele budou používat přístupová oprávnění `UNKNOWN`.

Informace o použití protokolu LDAP naleznete v příručce “Nastavení oprávnění” na stránce 402 .

ID uživatelů mohou obsahovat až 12 znaků a názvy skupin až 12 znaků.

Windows **Systémy Windows**

Seznamy ACL jsou založeny na ID uživatelů a skupinách. Kontroly jsou stejné jako u AIX and Linux. V různých doménách můžete mít různé uživatele se stejným ID uživatele. IBM MQ povoluje, aby ID uživatelů byla kvalifikována jménem domény, takže těmto uživatelům mohou být poskytnuty různé úrovně přístupu.

Název skupiny může volitelně zahrnovat název domény, uvedený v následujících formátech:

```
GroupName@domain domain_name\group_name
```

Globální skupiny kontroluje OAM pouze ve dvou případech:

1. Oddíl zabezpečení správce front obsahuje nastavení: `GroupModel=GlobalGroups`. Viz Zabezpečení.
2. Správce front používá alternativní skupinu přístupů zabezpečení. Viz **crtmqm** .

ID uživatele mohou obsahovat až 20 znaků, názvy domén až 15 znaků a názvy skupin až 64 znaků.

OAM nejprve zkontroluje lokální databázi zabezpečení, pak databázi primární domény a nakonec databázi všech důvěryhodných domén. První zjištěné ID uživatele používá OAM pro kontrolu. Každé z těchto ID uživatelů může mít odlišná členství ve skupině na konkrétním počítači.

Některé řídicí příkazy (například **crtmqm**) mění oprávnění k objektům IBM MQ pomocí správce oprávnění objektu (OAM). OAM prohledá databáze zabezpečení v pořadí uvedeném v předchozím odstavci, aby určila oprávnění pro konkrétní ID uživatele. V důsledku toho může oprávnění určené OAM přepsat skutečnost, že ID uživatele je členem lokální skupiny mqm. Pokud například zadáte příkaz **crtmqm** z ID uživatele ověřeného pomocí řadiče domény, který má členství v lokální skupině mqm prostřednictvím globální skupiny, příkaz selže, pokud má systém lokálního uživatele se stejným jménem, který není v lokální skupině mqm.

Další informace o nastavení atributu **SecurityPolicy** v systému Windowsnaleznete v tématech Instalovatelné služby a Konfigurace oddílů autorizační služby v systému Windows.

Windows ***Identifikátory zabezpečení produktu Windows (SID)***

Produkt IBM MQ v systému Windows používá SID, kde je k dispozici. Pokud není Windows SID dodán s autorizačním požadavkem, produkt IBM MQ identifikuje uživatele na základě samotného jména uživatele, ale to může mít za následek udělení chybného oprávnění.

V systému Windows se identifikátor zabezpečení (SID) používá k doplnění ID uživatele. Identifikátor SID obsahuje informace identifikující úplné podrobnosti o účtu uživatele na databázi správce účtů zabezpečení produktu Windows (SAM), kde je uživatel definován. Je-li vytvořena zpráva v systému IBM MQ for Windows, produkt IBM MQ ukládá identifikátor SID v deskriptoru zpráv. Když produkt IBM MQ na systému Windows provádí kontroly autorizace, použije identifikátor SID k získání dotazu na úplné informace z databáze SAM. (Databáze SAM, v níž je uživatel definován, musí být přístupná pro tento dotaz, aby byl úspěšný.)

By default, if a Windows SID is not supplied with an authorization request, IBM MQ identifies the user based on the user name alone. To 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 předejít, zahrňte do každého požadavku na autorizaci identifikátor SID; identifikátor SID je použit produktem IBM MQ k vytvoření pověření uživatele.

Chcete-li uvést, že všechny požadavky na autorizaci musí zahrnovat SID, použijte **regedit**. Nastavte SecurityPolicy na 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 . Tento příkaz se nazývá *oprávnění alternativního uživatele*a můžete jej použít na libovolném objektu IBM MQ .

Oprávnění alternativního uživatele je nezbytné, pokud server přijímá požadavky od programu a chce se ujistit, že má program požadované oprávnění pro tento požadavek. Server může mít požadované oprávnění, ale musí vědět, zda má tento program oprávnění pro akce, které požadoval.

Předpokládejme například, že serverový program spuštěný pod ID uživatele PAYSERV načte zprávu požadavku z fronty, která byla vložena do fronty, pomocí ID uživatele USER1. Když serverový program získá zprávu požadavku, zpracuje požadavek a vrátí odpověď zpět do fronty pro odpověď, která je uvedena spolu se zprávou požadavku. Server může namísto použití vlastního ID uživatele (PAYSERV) autorizovat otevření fronty pro odpověď. Server může v tomto případě určit jiné ID uživatele, USER1. V tomto příkladu můžete použít alternativní oprávnění k řízení, zda má PAYSERV povoleno zadat USER1 jako alternativní ID uživatele při otevření fronty pro odpověď.

ID alternativního uživatele je určeno v poli **AlternateUserId** deskriptoru objektu.

Linux Řešení některých problémů s členstvím ve skupinách v produktu Linux

Některé systémy se pomalu vracejí informace o skupině přes běžnou řadu volání rozhraní API operačního systému **getgrent** a pokud má váš podnik tisíce prohledávaných skupin a hledají skupiny, v nichž je uživatel `mqm` , může pomalý odezva způsobit vypršení interního časového limitu správce front. Chcete-li tento problém obejít, je k tomu alternativní rozhraní API operačního systému.

Chcete-li použít alternativní rozhraní API, které je rychlejší, a vrátí všechny skupiny z jednoho volání, nastavte proměnnou prostředí MQS_GETGROUPLIST_API.

Možná jste obdrželi chybu RC2035 při udělování připojení k sekundární skupině uživatele a povolení proměnné MQS_GETGROUPLIST_API zmírňuje problém.

IBM MQ pak místo rozhraní API **getgrent** používá rozhraní API produktu **getgrouplist** .

Chcete-li povolit **getgrouplist**:

1. Zastavit správce front
2. Vydejte příkaz pro export příkazu MQS_GETGROUPLIST_API=1 .
3. Restartujte správce front.

Zopakujte scénář, který selhal, a pokud byl váš problém vyřešen, můžete zvážit úpravu souboru `.bashrc / .profile` pro uživatele `mqm` a přidat tuto proměnnou prostředí, nebo přidat proměnnou prostředí do skriptu, který používáte ke spuštění správce front.

Pokud systém sloučí informace o uživateli nebo skupině pro operační systém z více úložišť, jako je služba NIS nebo LDAP, zajistěte, aby ID skupiny nebo uživatele byly konzistentní ve všech úložištích včetně lokálního úložiště, protože tyto informace se používají pro 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 .

Informace o volbách kontextu viz Informace o řízení kontextu a Přehled pro MQMD , kde jsou uvedeny popisy polí deskriptoru zpráv souvisejících s kontextem.

Implementace řízení přístupu v uživatelských procedurách zabezpečení

Řízení přístupu můžete implementovat v rámci uživatelské procedury zabezpečení pomocí MCAUserIdentifier nebo správce oprávnění k objektu.

MCAUserIdentifier

Každá instance kanálu, která má aktuální instanci, má přidruženou strukturu definice kanálu, MQCD. Počáteční hodnoty polí v produktu 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 ekvivalentní hodnotě MCAUSER, pokud je definice kanálu vytvořena jiným způsobem.

Struktura MQCD je předána výstupnímu programu kanálu, pokud je volána programem MCA. Je-li uživatelská procedura pro zabezpečení volána prostřednictvím programu MCA, může uživatelská procedura zabezpečení změnit hodnotu parametru *MCAUserIdentifier*a nahradit jakoukoli hodnotu zadanou v definici kanálu.

Multi On Multiplatforms, unless the value of *MCAUserIdentifier* is blank, the queue manager uses the value of *MCAUserIdentifier* as the user ID for authority checks when an MCA attempts to access the queue manager's resources after it has connected to the queue manager. Je-li hodnota *MCAUserIdentifier* prázdná, použije správce front výchozí ID uživatele MCA. Toto platí pro kanály RCVR, RQSTR, CLUSRCVR a SVRCONN. Pro odeslání MCA je výchozí ID uživatele vždy použito pro kontrolu oprávnění, i když hodnota *MCAUserIdentifier* není prázdná.

z/OS V systému z/OSmůže správce front použít hodnotu *MCAUserIdentifier* pro kontroly oprávnění, pokud tato hodnota není prázdná. For receiving MCAs and server connection MCAs, whether the queue manager uses the value of *MCAUserIdentifier* for authority checks depends on:

- Hodnota parametru PUTAUT v definici kanálu
- Profil produktu RACF použitý pro kontroly

- Úroveň přístupu ID uživatele adresního prostoru iniciátoru kanálu do profilu RESLEVEL

Pro posílání MCA to závisí na:

- Zda je odesílající agent MCA volajícím nebo respondentem
- Úroveň přístupu ID uživatele adresního prostoru iniciátoru kanálu do profilu RESLEVEL

ID uživatele, které se ukládá do úložiště uživatelské procedury zabezpečení v *MCAUserIdentifier* , lze získat různými způsoby. Několik příkladů:

- Pokud na konci klienta kanálu MQI neexistuje žádná uživatelská procedura zabezpečení, ID uživatele přidružené k aplikačním aplikacím klienta produktu IBM MQ přechází z klienta MCA pro připojení klienta do kanálu MCA připojení k serveru, když aplikace klienta odešle volání MQCONN.Agent MCA pro připojení k serveru ukládá toto ID uživatele do pole *RemoteUserIdentifier* ve struktuře definice kanálu, MQCD. Je-li hodnota *MCAUserIdentifier* prázdná, v prostředí MCA se uloží stejné ID uživatele v *MCAUserIdentifier*. Pokud agent MCA neukládá ID uživatele v souboru *MCAUserIdentifier*, může uživatelská procedura zabezpečení provést tuto akci později nastavením *MCAUserIdentifier* na hodnotu *RemoteUserIdentifier*.

  Pokud ID uživatele, které teče ze systému klienta, vstupuje do nové domény zabezpečení a není v systému serveru platné, může uživatelská procedura zabezpečení nahradit ID uživatele, která je platná, a uložit nahrazené ID uživatele v souboru *MCAUserIdentifier*.
- ID uživatele může být odesláno uživatelskou procedurou zabezpečení ochrany dat ve zprávě zabezpečení.

  Na kanálu zpráv může uživatelská procedura zabezpečení odesílající odesílající agent MCA odeslat ID uživatele, pod kterým je odesílající agent MCA spuštěn. Uživatelská procedura zabezpečení volaná přijímajícím agentem MCA může poté uložit ID uživatele do souboru *MCAUserIdentifier*. Podobně na kanálu MQI může uživatelská procedura zabezpečení na straně klienta kanálu odeslat ID uživatele přidružené k aplikaci produktu IBM MQ MQI client . Uživatelská procedura zabezpečení na konci serveru kanálu pak může uložit ID uživatele do souboru *MCAUserIdentifier*. Stejně jako v předchozím příkladu, pokud ID uživatele není platné na cílovém systému, může uživatelská procedura zabezpečení nahradit ID uživatele platnou a uložit nahrazené ID uživatele v souboru *MCAUserIdentifier*.

  Je-li jako součást identity a ověřovací služby přijat digitální certifikát, může uživatelská procedura pro zabezpečení mapovat rozlišující název v certifikátu na ID uživatele, které je platné na cílovém systému. Pak může uložit ID uživatele do *MCAUserIdentifier*.
- Je-li na kanálu použit TLS, je rozlišující název (DN) partnera předán do uživatelské procedury v poli SSLPeerNamePtr MQCD a DN vydavatele tohoto certifikátu je předáno do uživatelské procedury v poli Ptr SSLRemCertIssNameMQCXP.

Další informace o poli *MCAUserIdentifier* , struktury definice kanálu, MQCD a struktuře parametrů uživatelské procedury kanálu MQCXP najdete v tématu Volání uživatelské procedury kanálu a datové struktury. Další informace o ID uživatele, které teče z klientského systému na kanál MQI, najdete v tématu Řízení přístupu.

Poznámka: Aplikace uživatelské procedury zabezpečení postavené před vydáním produktu IBM WebSphere MQ 7.1 mohou vyžadovat aktualizaci. Další informace najdete v tématu Uživatelské programy zabezpečení kanálu.

Ověření uživatele správce oprávnění objektu IBM MQ

V případě IBM MQ MQI client připojení lze k úpravě nebo vytvoření struktury MQCSP použité v ověření uživatele správce oprávnění k objektu (OAM) použít uživatelské procedury zabezpečení. To je popsáno v tématu Programy výstupního bodu kanálů pro kanály systému zpráv

Implementace řízení přístupu ve výstupních procedurách zprávy

Může být nutné použít uživatelskou proceduru pro nahrazení jednoho ID uživatele jiným.

Uvažte aplikaci klienta, která odešle zprávu do serverové aplikace. 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 v zastoupení klienta.

Je-li parametr PUTAUT nastaven na CTX (nebo ALTMCA na systému z/OS) V definici kanálu se ID uživatele v poli *UserIdentifier* každé příchozí zprávy používá pro kontrolu oprávnění, když agent MCA otevře cílovou frontu.

Za určitých okolností se při generování zprávy o sestavě použije oprávnění ID uživatele v poli *UserIdentifier* zprávy způsobující tuto sestavu. Zejména sestavy potvrzení o doručení (COD) a sestavy o vypršení platnosti jsou vždy s tímto oprávněním zavedeny.

Vzhledem k těmto situacím může být nezbytné nahradit jedno ID uživatele pro jinou v poli *UserIdentifier* , protože zpráva vstoupí do nové domény zabezpečení. To lze provést ukončení zprávy na přijímajícím 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, který odeslal zprávu, může uživatelská procedura zprávy ověřit certifikát a mapovat rozlišující název v certifikátu na ID uživatele, které je platné na přijímajícím systému. Pak může nastavit pole *UserIdentifier* v deskriptoru zpráv na toto ID uživatele.

Je-li nezbytné pro ukončení zprávy změnit hodnotu pole *UserIdentifier* v příchozí zprávě, může být vhodné pro ukončení zprávy ověřit odesílatele zprávy ve stejnou dobu. Další informace naleznete v tématu “Mapování identit ve výstupních procedurách zprávy” na stránce 328.

Implementace řízení přístupu ve výstupu rozhraní API a ukončení přeletu rozhraní API

Rozhraní API nebo uživatelská procedura překřížení rozhraní API může poskytnout řízení přístupu k doplnění položek poskytovaného produktem IBM MQ. Ukončení může poskytovat řízení přístupu na úrovni zpráv. Uživatelská procedura může zajistit, že aplikace bude umístěna do fronty nebo se dostane 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, rozhraní API nebo výstupní bod rozhraní API může zkontrolovat, zda celková hodnota objednávky je menší než stanovená mezní hodnota.
- Zprávy dorazí do cílové fronty ze vzdálených správců front. Když se aplikace pokusí získat zprávu z fronty, rozhraní API nebo uživatelská procedura rozhraní API může zkontrolovat, zda je odesilatel zprávy autorizován k odeslání zprávy do fronty.

Multi V 9.2.3 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:

Chyba TBD

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

Multi Autorizace LDAP

Oprávnění LDAP můžete použít k odebrání potřeby lokálního ID uživatele.

Dostupnost oprávnění LDAP na podporovaných platformách

Autorizace LDAP je k dispozici na více platformách:

Upozornění:

Z obecné dostupnosti IBM MQ 9.0 je tato funkčnost dostupná na všech správcích front, ať již nových nebo migrovaných z předchozí verze.

Přehled autorizace LDAP

Při autorizaci LDAP mohou příkazy, které obsluhují konfiguraci autorizace, jako jsou **setmqaut** a **DISPLAY AUTHREC**, zpracovat Rozlišující názvy. Dříve byli uživatelé ověřováni porovnáním jejich 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, spíše než rozlišující název, bude ID uživatele zpracováno. Je-li například na kanálu s parametrem PUTAUT (CTX) příchozí zpráva, jsou znaky v ID uživatele mapovány na rozlišující název služby LDAP a jsou provedeny příslušné kontroly autorizace.

Další příkazy jako např. **DISPLAY CONN**, pokračují v práci a zobrazují skutečnou hodnotu pro ID uživatele, i když toto ID uživatele nemusí ve skutečnosti existovat na lokálním OS.

Linux AIX Je-li autorizace LDAP na místě, správce front vždy použije 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 kohokoli jiného, kdo patří do jakékoli skupiny uživatelů.

Stejně jako u modelu OS má uživatel stále kombinované oprávnění, které bylo přiřazeno jak k jednotlivému, tak ke všem skupinám (pokud existují), ke kterému uživatel patří.

Předpokládejme například, že v úložišti LDAP byly definovány následující záznamy.

- 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 relevantní atributy pro rozeznání 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 dokončit pole CSPUserID , které se používá ve volání MQCNO, s některou 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 zadané hodnoty k ověření kontextu operačního systému " jodoe".

Multi Nastavení oprávnění

Jak použijete krátký název nebo **USRFIELD** k nastavení autorizací.

Přístup k práci s více formáty, jak je popsáno v “Autorizace LDAP” na stránce 401, pokračuje do autorizačních příkazů s dalším rozšířením, které lze použít v nezdobeném módu buď pro `shortname` , nebo pro USRFIELD.

Znakový řetězec uvádí konkrétní atribut v záznamu LDAP, když pojmenováváte uživatele (činitele) pro autorizaci.

Důležité: Znakový řetězec nesmí obsahovat znak = , protože tento znak nemůže být použit v ID uživatele operačního systému.

Předáte-li OAM základní jméno pro autorizaci, která je potencionálně `shortname`, musí se znakový řetězec vejít do 12 znaků. Algoritmus mapování se nejprve pokusí o jeho vyřešení na DN pomocí atributu SHORTUSR ve svém dotazu LDAP.

Pokud to selže s chybou UNKNOWN_ENTITY nebo pokud daný řetězec nemůže být `shortname`, je proveden další pokus pomocí atributu USRFIELD k vytvoření dotazu LDAP.

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 72. Nastavení autorizace uživatele

Příkaz	**Poznámka**
`setmqaut -m QM -t qmgr -p jodoe +connect`	Jedná se o plochý, nekvalifikovaný název, vyřešený prostřednictvím SHORTUSR.
`setmqaut -m QM -t qmgr -pJohnDoe1@yourcompany.com +connect`	Také plochý, nekvalifikovaný název, který řeší přes USRFIELD na stejnou entitu.
`setmqaut -m QM -t qmgr -p email=JohnDoe1@yourcompany.com +connect`	Použití pojmenovaného atributu.
`setmqaut -m QM -t qmgr -p "phone=1234567" +connect`	Použití jiného pojmenovaného atributu, který nemusí být žádným z hodnot nakonfigurovaných na objektu AUTHINFO.

Jako alternativu k příkazu **setmqaut** můžete použít příkaz MQSC SET AUTHREC :

```
SET AUTHREC OBJTYPE(QMGR) PRINCIPAL('JohnDoe1@yourcompany.com') AUTHADD(connect)
```

nebo příkaz Set Authority Record (MQCMD_SET_AUTHRE/REC) PCF s prvkem MQCACF_PRINCIP_ENTITY_NAMES, který obsahuje řetězec:

```
 "cn=JohnDoe,ou=users,o=yourcompany,c=yourcountry"
```

Při zpracování skupin se nevyskytuje žádná nejednoznačnost zpracování `shortname` , protože neexistuje požadavek na přizpůsobení jakékoli formy názvu skupiny do 12 znaků. Proto neexistuje ekvivalent atributu SHORTUSR pro skupiny.

To znamená, že příklady syntaxe popsané v Tabulka 73 na stránce 404 jsou platné, za předpokladu, že jste nakonfigurovali objekt AUTHINFO s rozšířenými atributy a nastavili:

```
GRPFIELD(longname)
BASEDNG(ou=groups,o=yourcompany,c=yourcountry ) CLASSGRP(groupOfNames)
```

Tabulka 73. 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 úplných DN

Jako alternativu k předcházejícímu příkazu **setmqaut** můžete použít příkaz MQSC SET AUTHREC :

```
SET AUTHREC OBJTYPE(QMGR) GROUP('ApplicationGroupA')
      AUTHADD(connect)
```

nebo příkaz Set Authority Record (MQCMD_SET_AUTHREC) PCF s prvkem MQCACF_GROUP_ENTITY_NAMES obsahujícím řetězec:

```
 "ApplicationGroupA"
```

Důležité:

Kterýkoli formát, který použijete k odkazování na jméno, ať už pro uživatele nebo skupinu, musí být možné odvodit jedinečné DN.

Takže například nesmíte mít dva různé záznamy, které mají oba "`shortu=jodoe`".

Pokud nelze určit jednotlivé jedinečné DN, vrátí objekt OAM MQRC_UNKNOWN_ENTITY.

Multi Zobrazení autorizací

Různé metody zobrazení autorizace uživatelů nebo skupin.

příkaz dspmqaut

Nejjednodušší metodou zobrazení autorizací dostupných pro uživatele nebo skupinu je použití příkazu dspmqaut .

Pro identifikaci uživatele nebo skupiny můžete použít dotaz na libovolné variace syntaxe. Všimněte si, že výstup příkazu opakuje identitu ve formátu uvedeném na příkazovém řádku. Výstup nehlásí úplný rozlišující název 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 určovat činitele nebo skupinu v kterémkoli z podporovaných formátů, jako jsou tabulky **setmqaut** popsané v části “Nastavení oprávnění” na stránce 402. Nicméně, na rozdíl od **dspmqaut**, příkaz **dmpmqaut** vždy nahlásí 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 na vybraných záznamech, vždy zobrazí úplné DN ve formátu, který lze přehrát později.

```
dmpmqcfg -m QM -x authrec
------------------------------------
SET AUTHREC PROFILE(SELF) +
    PRINCIPAL('cn=JohnDoe, ou=users, o=yourcompany, c=yourcountry') +
    OBJTYPE(QMGR)
    AUTHADD(CONNECT)
```

Multi

Další pokyny při použití autorizace LDAP

Stručný popis změn rozhraní MQI (Message Queue Interface) a dalších příkazů MQSC a PCF, o kterých byste měli být informováni při použití autorizace LDAP z produktu IBM MQ 9.0.0.

ADOPTCTX

Nejsou žádné požadavky na aplikace poskytující informace o ověření, nebo pro atribut ADOPTCTX , který má být nastaven na hodnotu YES.

Pokud se aplikace explicitně neověřuje, nebo je-li hodnota **ADOPTCTX** nastavena na NO pro aktivní objekt CONNAUTH, kontext identity přidružený k aplikaci je převzat z ID uživatele operačního systému.

Je-li třeba aplikovat autorizace, tento kontext se namapuje 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.

Jsou-li tato pole použita, je 12znakové ID uživatele mapováno na DN pomocí stejných pravidel, jako na příkazech **setmqaut**, **dmpmqaut**a **dspmqaut** .

MQPUT a MQPUT1 také umožňují vhodně autorizovaným programům nastavit pole MQMD UserIdentifier . Hodnota tohoto pole nebude během procesu PUT nastavena na police a lze ji nastavit na libovolnou hodnotu.

Jako obvykle však může být hodnota **UserIdentifier** použita pro autorizaci v pozdějších fázích zpracování zpráv, například když je na přijímajícím kanálu definován parametr PUTAUT (CTX).

V tomto okamžiku bude identifikátor zkontrolován kvůli autorizaci pomocí konfigurace přijímajícího správce front-což může být LDAP nebo založeno na technologii OSS.

Výstupní parametry pro volání MQI

Kdekoli je ID uživatele poskytnuto programu ve struktuře MQI, je to 12znaková verze krátkého názvu přidružená k připojení.

Například hodnota **MQAXC.UserId** pro rozhraní API Exits je krátký název vrácený z mapování LDAP.

Další administrativní příkazy MQSC a PCF

Příkazy, které zobrazují informace o uživateli ve stavu objektu, například DISPLAY CONN USERID vracejí 12znakový krátký název přidružený k danému kontextu. Úplné DN se nezobrazí.

Příkazy, které umožňují deklaraci identit, jako např. mapovací pravidla CHLAUTH nebo hodnoty MCAUSER pro kanály, mohou převzít hodnoty až do maximální délky definované pro tyto atributy (momentálně 64 znaků).

Syntaxe není nijak změněna. Je-li pro tuto identitu požadováno oprávnění, je interně mapováno 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 (jedoe)* pro všechna připojení.

Multi Přepínání mezi modely autorizace OS a LDAP

Jak přepínáte mezi různými metodami autorizace na různých platformách.

Atribut CONNAUTH pro správce front ukazuje na objekt AUTHINFO. Je-li objekt typu IDPWLDAP, použije se pro ověření úložiště LDAP.

Nyní můžete použít metodu autorizace na stejný objekt, který vám umožní pokračovat v autorizaci založené na operačním systému, nebo pracovat s autorizací LDAP

IBM i, AIX and Linux

IBM i Linux AIX

Správce front lze přepínat kdykoli mezi OS a modely LDAP. Konfiguraci můžete změnit a aktivovat ji tak, že použijete příkaz 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 OS a modely LDAP, správce front musí být restartován, aby se změna projevila. Jinak můžete provést změnu jako aktivní pomocí příkazu REFRESH SECURITY TYPE (CONNAUTH) .

Pravidla zpracování

Když přepínáte z OS na autorizaci LDAP, všechna existující pravidla oprávnění operačního systému, která byla nastavena, se stanou neaktivními a neviditelnými.

Příkazy jako např. **dmpmqaut** nezobrazují tato pravidla operačního systému. Podobně při přepnutí z LDAP na OS se všechny definované autorizace LDAP stanou neaktivními a neviditelnými, čímž se obnoví původní pravidla operačního systému.

Chcete-li zálohovat definice správce front z libovolného důvodu pomocí příkazu **dmpmqcfg** , bude tato záloha obsahovat pouze pravidla, která jsou definována pro autorizační metodu v platnosti v době zálohování.

Multi Administrace LDAP

Přehled o tom, jak každá platforma spravuje službu LDAP.

Při použití autorizace LDAP není členství ve skupině mqm (nebo ekvivalent) v operačním systému důležité. Členství v této skupině řídí pouze to, zda lze zpracovat určité příkazy příkazového řádku.

Konkrétně musíte být v této skupině, chcete-li vydat příkazy strmqm a endmqm .

Jakmile je správce front spuštěn, jsou nyní limity na plně privilegovaném účtu. Kromě ID uživatele osoby, která vydává příkaz **strmqm** , jiní uživatelé patřící do skupiny operačního systému mqm (nebo ekvivalentní skupiny) nemají speciální oprávnění.

Oprávnění ostatních uživatelů jsou založena na tom, do kterých skupin LDAP patří. Nekvalifikované použití názvu skupiny mqm v příkazech, jako například **setmqaut** , není povoleno mapovat na žádnou skupinu LDAP.

AIX and Linux

Linux AIX

Jakmile je správce front spuštěn, jediným automaticky privilegovaným účtem je skutečný uživatel, který spustil správce front.

ID mqm stále existuje a používá se jako vlastník prostředků operačního systému, jako jsou například soubory, protože mqm je efektivní ID, pod kterým je správce front spuštěn. Uživatel mqm však nebude automaticky schopen provádět administrativní úlohy řízené OAM.

Windows

Windows

V systému Windowsjsou automaticky plně privilegovanými účty uživatel operačního systému, který spustil správce front, a také uživatel, který spouští procesy správce front jádra, například MUSR_MQADMIN, pokud byl správce front spuštěn jako služba Windows .

Při spuštění v režimu autorizace LDAP se produkt Windows chová velmi podobně jako platformy AIX and Linux . Zabývá se dvanácti krátkými jmény a úplnými DN.

IBM i

IBM i

V systému IBM ijsou automaticky privilegované účty ta, která spouští správce front a ID QMQM.

Potřebujete obě ID, protože ID uživatele, které spouští správce front, je nezbytné pouze ke spuštění systému. Jakmile je správce front spuštěn, má 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 dodáván na platformách AIX and Linux jako:

```
MQ_INSTALLATION_PATH/samp/bin/amqauthg.sh
```

Tato ukázka má dva parametry:

- Název správce front
- Název skupiny LDAP

Ukázkové procesy používají příkazy setmqaut , které poskytují úplnou autoritu pro všechny objekty. Jedná se o stejný skript, který je generován průvodcem OAM produktu IBM MQ Explorer pro administrativní role. Například, kód začíná:

```
setmqaut -t q -m qmgr -n "**" +alladm -g
      groupname
```

Důvěrnost zpráv

Šifrované zprávy zajišťují, že obsah zpráv zůstane důvěrný. V produktu IBM MQ existují různé metody šifrování zpráv v závislosti na vašich potřebách.

Pokud potřebujete ochranu dat na úrovni koncových bodů pro vaši dvoubodovou infrastrukturu systému zpráv, můžete použít produkt Advanced Message Security k šifrování zpráv nebo napsat vlastní uživatelskou proceduru rozhraní API nebo uživatelskou proceduru pro přechod na rozhraní API.

Nejbezpečnější řešení je poskytovat šifrování konce do konce, zašifrováním zprávy z bodu, který je vložen aplikací, do bodu, kde je aplikace spotřebovávající aplikací. To lze provést pomocí “Plánování pro databázi Advanced Message Security” na stránce 102 (AMS) nebo tím, že napíšete vlastní uživatelskou proceduru rozhraní API nebo uživatelskou proceduru pro přechod rozhraní API; další informace viz “Implementace utajení v uživatelských ukončovacích programech” na stránce 456 .

Pokud potřebujete šifrovat zprávy pouze během přenosu po síti, můžete použít TLS; viz “Protokoly zabezpečení TLS v produktu IBM MQ” na stránce 22 , kde získáte další informace, nebo můžete napsat vlastní uživatelskou proceduru pro zabezpečení zprávy, ukončit zprávu nebo odeslat a přijmout výstupní programy, abyste mohli provést šifrování.

z/OS V 9.2.0 Pokud potřebujete šifrovat zprávy ve zbytku správce front, můžete v daném správci front použít šifrování dat produktu z/OS ; viz Utajení dat ve zbytku na IBM MQ for z/OS s šifrováním datové sady. Další informace viz.

Související úlohy

Připojení dvou správců front pomocí protokolu TLS

Bezpečná připojení klienta ke správci front

Povolení CipherSpecs

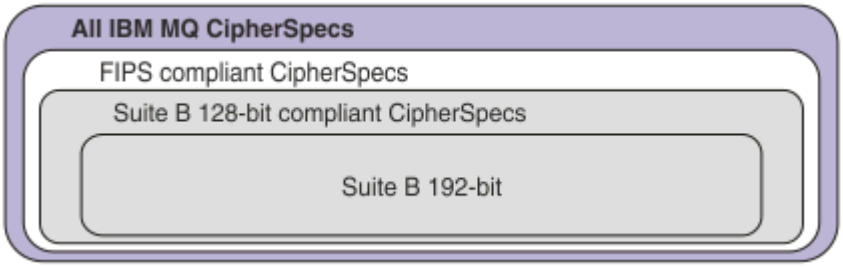
Povolte CipherSpec pomocí parametru **SSLCIPH** v příkazu **DEFINE CHANNEL** nebo **ALTER CHANNEL** MQSC.

Poznámka: V systému AIX, Linux, and Windowsposkytuje produkt IBM MQ kompatibilitu se standardem FIPS 140-2 prostřednictvím šifrovacího modulu "IBM Crypto for C" . Certifikát pro tento modul byl přesunut do historického stavu. Zákazníci by si měli prohlédnout IBM Crypto for C certificate a měli by si být vědomi jakýchkoli 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 9.2.0 V 9.2.0 V produktu IBM MQ 9.2.0produkt podporuje protokol zabezpečení TLS 1.3 na všech platformách. z/OS V systému IBM MQ for z/OSje protokol TLS 1.3 podporován pouze v systému z/OS 2.4 nebo novějším.

CipherSpecs , které můžete použít pro každou z těchto platforem, jsou uvedeny v části Tabulka 74 na stránce 410. Informace o použití těchto specifikací CipherSpecsnaleznete v části “Použití TLS 1.3 v IBM MQ” na stránce 413 a “IBM MQ MQI client a TLS 1.3” na stránce 413.

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 74 na stránce 410. Další informace o migraci pro použití aliasu CipherSpecnaleznete v tématu Migrace existujících konfigurací zabezpečení pro použití aliasu CipherSpec.

V 9.2.0 Můžete nakonfigurovat výchozí CipherSpecs , jak je popsáno v tématu “Výchozí hodnoty CipherSpec jsou povoleny v produktu IBM MQ” na stránce 414. 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 422.
- 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 423.

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 424. Informace o povolení zamítnutých specifikací CipherSpecsviz “Povolení zamítnutých specifikací CipherSpecs na systému IBM MQ for Multiplatforms” na stránce 427 nebo “Povolení zamítnutých specifikací CipherSpecs na systému z/OS” na stránce 428.

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 74. Specifikace šifrování, které lze použít s podporou TLS produktu IBM MQ

Podpora platformy "1" na stránce 412	Název specifikace šifrování	Hexadecimální kód	Použitý protokol	Algoritmus MAC	Šifrovací algoritmus (šifrovací bity)	FIPS "2" na stránce 412	Suite B
Specifikace CipherSpecs aliasu							
Vše	ANY_TLS13_OR_HIGHER "3" na stránce 412 "4" na stránce 412 "5" na stránce 412	Není k dispozici	Dohodnuto	Dohodnuto	Dohodnuto	Dohodnuto	Dohodnuto
Vše	ANY_TLS13 "4" na stránce 412 "5" na stránce 412 "6" na stránce 412	Není k dispozici	TLS 1.3	Dohodnuto	Dohodnuto	Dohodnuto	Dohodnuto
Vše	ANY_TLS12_OR_HIGHER "4" na stránce 412 "5" na stránce 412 "7" na stránce 412	Není k dispozici	Dohodnuto	Dohodnuto	Dohodnuto	Dohodnuto	Dohodnuto
Vše	ANY_TLS12 "8" na stránce 412	Není k dispozici	TLS 1.2	Dohodnuto	Dohodnuto	Dohodnuto	Dohodnuto
Vše	ANY "9" na stránce 412	Není k dispozici	Dohodnuto	Dohodnuto	Dohodnuto	Dohodnuto	Dohodnuto
CipherSpecs pro TLS 1.3							
Vše	TLS_AES_128_GCM_SHA256 "4" na stránce 412	1301	TLS 1.3	GCM	AES-128 s volbou GCM (128)	Ano	Ne
Vše	TLS_AES_256_GCM_SHA384 "4" na stránce 412	1302	TLS 1.3	GCM	AES-256 s GCM (256)	Ano	Ne
Vše	TLS_CHACHA20_POLY1305_SHA256 "4" na stránce 412	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
ALW	TLS_AES_128_CCM_8_SHA256 "11" na stránce 412	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 "10" na stránce 412	003C	TLS 1.2	SHA-256	AES (128)	Ano	Ne
Vše	TLS_RSA_WITH_AES_256_CBC_SHA256 "10" na stránce 412 "12" na stránce 412	003D	TLS 1.2	SHA-256	AES (256)	Ano	Ne
Vše	TLS_RSA_WITH_AES_128_GCM_SHA256 "10" na stránce 412 "13" na stránce 412	009C	TLS 1.2	SHA-256 a AEAD GCM	AES (128)	Ano	Ne

Tabulka 74. Specifikace šifrování, které lze použít s podporou TLS produktu IBM MQ (pokračování)

Podpora platformy "1" na stránce 412	Název specifikace šifrování	Hexadecimální kód	Použitý protokol	Algoritmus MAC	Šifrovací algoritmus (šifrovací bity)	FIPS "2" na stránce 412	Suite B
Vše	TLS_RSA_WITH_AES_256_GCM_SHA384 "10" na stránce 412 "12" na stránce 412 "13" na stránce 412	009D	TLS 1.2	SHA-384 a AEAD GCM	AES (256)	Ano	Ne
Vše	ECDHE_ECDSA_AES_128_CBC_SHA256 "10" na stránce 412	C023	TLS 1.2	SHA-256	AES (128)	Ano	Ne
Vše	ECDHE_ECDSA_AES_256_CBC_SHA384 "10" na stránce 412 "12" na stránce 412	C024	TLS 1.2	SHA-384	AES (256)	Ano	Ne
Vše	ECDHE_RSA_AES_128_CBC_SHA256 "10" na stránce 412	C027	TLS 1.2	SHA-256	AES (128)	Ano	Ne
Vše	ECDHE_RSA_AES_256_CBC_SHA384 "10" na stránce 412 "12" na stránce 412	C028	TLS 1.2	SHA-384	AES (256)	Ano	Ne
Multi	ECDHE_ECDSA_AES_128_GCM_SHA256 "12" na stránce 412 "13" na stránce 412	C02B	TLS 1.2	SHA-256 a AEAD GCM	AES (SHA384)	Ano	128bitové
Multi	ECDHE_ECDSA_AES_256_GCM_SHA384 "12" na stránce 412 "13" na stránce 412	C02C	TLS 1.2	SHA-384 a AEAD GCM	AES (SHA384)	Ano	192bitové
Vše	ECDHE_RSA_AES_128_GCM_SHA256 "13" na stránce 412	C02F	TLS 1.2	SHA-256 a AEAD GCM	AES (128)	Ano	Ne
Vše	ECDHE_RSA_AES_256_GCM_SHA384 "12" na stránce 412 "13" na stránce 412	C030	TLS 1.2	AEAD AES-128 GCM	AES (SHA384)	Ano	Ne

Tabulka 74. Specifikace šifrování, které lze použít s podporou TLS produktu IBM MQ (pokračování)

Podpora platformy "1" na stránce 412	Název specifikace šifrování	Hexadecimální kód	Použitý protokol	Algoritmus MAC	Šifrovací algoritmus (šifrovací bity)	FIPS "2" na stránce 412	Suite B

Notes:

1. Seznam platforem pokrytých každou ikonou platformy viz Vydání a ikony platformy v dokumentaci 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. z/OS Chcete-li použít protokol TLS 1.3 nebo LIBOVOLNOU specifikaci CipherSpec na systému IBM MQ for z/OS, musí mít operační systém verzi z/OS 2.4 nebo novější.
5. 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.
6. 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.
7. 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.
8. Specifikace ANY_TLS12 CipherSpec představuje podmnožinu přijatelných specifikací CipherSpecs, které používají protokol TLS 1.2, jak je uvedeno v této tabulce pro jednotlivé platformy.
9. ALW Alias ANY šifrování CipherSpec vyjedná nejvyšší úroveň zabezpečení, kterou vzdálený konec umožní.
10. IBM i Tyto specifikace CipherSpecs nejsou povoleny v systémech IBM i 7.4, které mají hodnotu systému QSSLCSLCTL nastavenou na *OPSSYS.
11. ALW Tato šifrování CipherSpecs používají 8oktetovou hodnotu ICV (8-octet Integrity Check Value) namísto 16oktetové hodnoty ICV.
12. 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.
13. Windows Linux 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 V 9.2.0 V 9.2.0 Upravte datovou sadu QMINI správce front a změňte nastavení vlastnosti **AllowTLSV13** na:

```
TransportSecurity:
    AllowTLSV13=FALSE
```

IBM MQ MQI client a TLS 1.3

V 9.2.0 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 43
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 17
Kryptografické bezpečnostní protokoly musí souhlasit s algoritmem používaným zabezpečeným připojením. CipherSpecs a CipherSuites definují specifické kombinace algoritmů.

“Konfigurace produktu IBM MQ pro sadu B” na stránce 41
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 31
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, GSKit. V případě aplikací knihovny C a nespravované knihovny .NET používají GSKit pro šifrovací funkčnost. Implementace šifrovacích algoritmů AES-GCM podle 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.

V 9.2.0 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 408.

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.

V 9.2.0 V 9.2.0 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 75. 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

Tabulka 75. Pořadí CipherSpecs od IBM MQ 9.2.0 (pokračování)				
Platforma	**CipherSpec**	**Protokol**	**Hexadecimální kód**	**Standardně povoleno**
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
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

Tabulka 75. Pořadí CipherSpecs od IBM MQ 9.2.0 (pokračování)				
Platforma	**CipherSpec**	**Protokol**	**Hexadecimální kód**	**Standardně povoleno**
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
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

Tabulka 75. Pořadí CipherSpecs od IBM MQ 9.2.0 (pokračování)				
Platforma	**CipherSpec**	**Protokol**	**Hexadecimální kód**	**Standardně povoleno**
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
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 76. 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
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

Tabulka 76. CipherSpecs objednat před IBM MQ 9.2.0 (pokračování)			
Platforma	**CipherSpec**	**Protokol**	**Standardně povoleno**
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
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

Tabulka 76. CipherSpecs objednat před IBM MQ 9.2.0 (pokračování)			
Platforma	**CipherSpec**	**Protokol**	**Standardně povoleno**
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
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_AE
S_256_CBC_SHA384,ECDHE_RSA_AES_128_CBC_SHA256,ECDHE_RSA_AES_256_CBC_SHA384,ECDHE_ECDSA_AES_128_G
CM_SHA256,ECDHE_ECDSA_AES_256_GCM_SHA384,ECDHE_RSA_AES_128_GCM_SHA256,ECDHE_RSA_AES_256_GCM_SHA3
84
```

Poskytnutí vlastního seznamu seřazených a povolených CipherSpecs na systému IBM MQ for Multiplatforms

Multi

Je možné, abyste poskytli alternativní sadu souborů CipherSpecs , které jsou povoleny a v pořadí, v jakém jsou upřednostňovány pro použití s kanály IBM MQ , buď pomocí atributu ALW proměnná prostředí **AMQ_ALLOWED_CIPHERS** , nebo atributu sekce SSL **AllowedCipherSpecs** souboru `.ini` . Toto nastavení můžete použít z jednoho z následujících důvodů:

- 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 `ALL`představující 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

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 `ALL`představující 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 428.

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.

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" . Certifikát pro tento modul byl přesunut do historického stavu. Zákazníci by si měli prohlédnout IBM Crypto for C certificate a měli by si být vědomi jakýchkoli 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 427 nebo “Povolení zamítnutých specifikací CipherSpecs na systému z/OS” na stránce 428.

Zamítnuté specifikace CipherSpecs , které můžete použít s podporou protokolu IBM MQ TLS, jsou uvedeny v následující tabulce.

Tabulka 77. Zamítnuté specifikace CipherSpecs můžete znovu povolit pro použití s produktem IBM MQ.

Podpora platformy “1” na stránce 427	Název specifikace šifrování	Hexadecimální kód	Použitý protokol	Integrita dat	Šifrovací algoritmus (šifrovací bity)	FIPS “2” na stránce 427	Suite B	Aktualizovat při zamítnutí
CipherSpecs pro SSL 3.0								
IBM i	AES_SHA_US “3” na stránce 427	002F	SSL 3.0	SHA-1	AES (128)	Ne	Ne	9.0.0.0
Vše	DES_SHA_EXPORT “3” na stránce 427 “4” na stránce 427 “5” na stránce 427	0005	SSL 3.0	SHA-1	DES (56)	Ne	Ne	9.0.0.0
ALW	DES_SHA_EXPORT1024 “3” na stránce 427 “6” na stránce 427	0062	SSL 3.0	SHA-1	DES (56)	Ne	Ne	9.0.0.0
ALW	FIPS_WITH_DES_CBC_SHA “3” na stránce 427	FEFE	SSL 3.0	SHA-1	DES (56)	Ne“7” na stránce 427	Ne	9.0.0.0
ALW	FIPS_WITH_3DES_EDE_CBC_SHA “3” na stránce 427	FEFF	SSL 3.0	SHA-1	3DES (168)	Ne“8” na stránce 427	Ne	9.0.0.1 a 9.0.1
Vše	NULL_MD5 “3” na stránce 427	0001	SSL 3.0	MD5	Není	Ne	Ne	9.0.0.1
Vše	NULL_SHA “3” na stránce 427	0002	SSL 3.0	SHA-1	Není	Ne	Ne	9.0.0.1
Vše	RC2_MD5_EXPORT “3” na stránce 427 “4” na stránce 427 “5” na stránce 427	0006	SSL 3.0	MD5	RC2 (40)	Ne	Ne	9.0.0.0

Tabulka 77. Zamítnuté specifikace CipherSpecs můžete znovu povolit pro použití s produktem IBM MQ. (pokračování)

Podpora platformy "1" na stránce 427	Název specifikace šifrování	Hexadecimální kód	Použitý protokol	Integrita dat	Šifrovací algoritmus (šifrovací bity)	FIPS "2" na stránce 427	Suite B	Aktualizovat při zamítnutí
Vše	RC4_MD5_EXPORT "4" na stránce 427 "3" na stránce 427	0003	SSL 3.0	MD5	RC4 (40)	Ne	Ne	9.0.0.0
Vše	RC4_MD5_US "3" na stránce 427	0004	SSL 3.0	MD5	RC4 (128)	Ne	Ne	9.0.0.0
Vše	RC4_SHA_US "3" na stránce 427 "5" na stránce 427	0005	SSL 3.0	SHA-1	RC4 (128)	Ne	Ne	9.0.0.0
ALW	RC4_56_SHA_EXPORT1024 "3" na stránce 427 "6" na stránce 427	0064	SSL 3.0	SHA-1	RC4 (56)	Ne	Ne	9.0.0.0
Vše	TRIPLE_DES_SHA_US "3" na stránce 427 "5" na stránce 427	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 427	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 427 "4" na stránce 427	0003	TLS 1.0	MD5	RC4 (40)	Ne	Ne	9.0.0.0
Vše	TLS_RSA_WITH_DES_CBC_SHA "3" na stránce 427	0005	TLS 1.0	SHA-1	DES (56)	Ne "9" na stránce 427	Ne	9.0.0.0
IBM i	TLS_RSA_WITH_NULL_MD5 "3" na stránce 427	0001	TLS 1.0	MD5	Není	Ne	Ne	9.0.0.1
IBM i	TLS_RSA_WITH_NULL_SHA "3" na stránce 427	0002	TLS 1.0	SHA-1	Není	Ne	Ne	9.0.0.1
IBM i	TLS_RSA_WITH_RC4_128_MD5 "3" na stránce 427	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 427	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 427 "10" na stránce 427	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 427	C006	TLS 1.2	SHA-1	Není	Ne	Ne	9.0.0.1
ALW	ECDHE_ECDSA_RC4_128_SHA256 "3" na stránce 427	C007	TLS 1.2	SHA-1	RC4 (128)	Ne	Ne	9.0.0.0

Tabulka 77. Zamítnuté specifikace CipherSpecs můžete znovu povolit pro použití s produktem IBM MQ. (pokračování)

Podpora platformy "1" na stránce 427	Název specifikace šifrování	Hexadecimální kód	Použitý protokol	Integrita dat	Šifrovací algoritmus (šifrovací bity)	FIPS "2" na stránce 427	Suite B	Aktualizovat při zamítnutí
ALW IBM i	ECDHE_RSA_NULL_SHA256 "3" na stránce 427	C010	TLS 1.2	SHA-1	Není	Ne	Ne	9.0.0.1
ALW IBM i	ECDHE_RSA_RC4_128_SHA256 "3" na stránce 427	C011	TLS 1.2	SHA-1	RC4 (128)	Ne	Ne	9.0.0.0
ALW	TLS_RSA_WITH_NULL_NULL "3" na stránce 427	0000	TLS 1.2	Není	Není	Ne	Ne	9.0.0.1
Vše	TLS_RSA_WITH_NULL_SHA256 "3" na stránce 427	003B	TLS 1.2	SHA-256	Není	Ne	Ne	9.0.0.1
ALW	TLS_RSA_WITH_RC4_128_SHA256 "3" na stránce 427	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 77. Zamítnuté specifikace CipherSpecs můžete znovu povolit pro použití s produktem IBM MQ. (pokračování)

Podpora platformy "1" na stránce 427	Název specifikace šifrování	Hexadecimální kód	Použitý protokol	Integrita dat	Šifrovací algoritmus (šifrovací bity)	FIPS "2" na stránce 427	Suite B	Aktualizovat při zamítnutí

Notes:

1. Seznam platforem pokrytých každou ikonou platformy viz Vydání a ikony platformy v dokumentaci 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. 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. 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 ALLpředstavující 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

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: V 9.2.0 V 9.2.0 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 43
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 nastavením aliasu CipherSpec

Tyto informace popisují očekávané chování s různými kombinacemi aliasu CipherSpecs v konfiguracích klienta a serveru. Zde klient odkazuje na entitu zahajující komunikaci, například na klientskou aplikaci nebo na odesílací kanál správce front a server odkazuje na entitu přijímající komunikaci od klienta, například kanál připojení serveru nebo kanál příjemce.

Minimální protokol versus pevný protokol CipherSpecs

V 9.2.0

Produkt IBM MQ podporuje dva různé typy specifikace CipherSpecs:

Minimální protokol
Minimální protokol CipherSpecs jsou ty, které nenastavují horní hranici, například ANY, ANY_TLS12_OR_HIGHER nebo ANY_TLS13_OR_HIGHER.

Pevný protokol
Pevný protokol CipherSpecs jsou ty, které identifikují specifický protokol, například ANY_TLS12 a ANY_TLS13, nebo specifický algoritmus, jako např. ECDHE_ECDSA_3DES_EDE_CBC_SHA256.

V systému IBM MQ 9.2.0jsou na všech platformách podporovány minimální a pevné protokoly CipherSpecs .

Chcete-li maximalizovat jednoduchost konfigurace při zachování zabezpečení, doporučuje se používat **minimální protokol** CipherSpecs na obou stranách kanálu. To umožňuje, aby vaše komunikace automaticky podporovala a používala vyšší verzi protokolu TLS, když obě strany podporují novou verzi bez nutnosti měnit konfiguraci obou stran.

Použití **minimálního protokolu** CipherSpec na straně iniciace, ale **pevný protokol** CipherSpec na přijímající straně může mít za následek zamítnutí připojení a

- Multi Zprávy AMQ9631 a AMQ9641 jsou vydávány.

- z/OS V 9.2.0 V 9.2.0 Vydávají se zprávy CSQX631E a CSQX641E .

Následující tabulky zobrazují vztah mezi různými nastaveními aliasu CipherSpec a očekávaným výsledkem. Tabulka 78 na stránce 430 ukazuje očekávané chování, pokud není TLS 1.3 povoleno na klientovi, serveru nebo obou. Tabulka 79 na stránce 430 ukazuje očekávané chování, je-li TLS 1.3 povoleno na klientovi i na serveru. V obou případech jsou CipherSpecs pro klienta zobrazeny na ose Y tabulky a CipherSpecs pro server jsou zobrazeny na ose X tabulky.

Poznámka: V následujících tabulkách označují buňky označené jako *Pravděpodobně selhání* potenciální konflikt, když uvedete **minimální protokol** CipherSpec pro jednu část připojení a specifický (**pevný protokol**) CipherSpec pro jinou část.

Předpokládejme například, že klient a server jsou nastaveny na použití LIBOVOLNÉ CipherSpeca kanál serveru je nastaven tak, aby používal specifickou specifikaci CipherSpec:

- Pokud nejsilnější podporovaná volba CipherSpec pro klienta i server odpovídá specifické sadě CipherSpec konfigurované v kanálu, úspěšně se vyřeší navázání komunikace TLS.
- Pokud však existuje silnější CipherSpec , kterou klient i server podporují, řeší se při navázání komunikace TLS, i když neodpovídá CipherSpec uvedenému v kanálu a komunikace výměnou potvrzení TLS selže.

Tabulka 78. Očekávané chování, když není TLS 1.3 povoleno na klientovi, serveru nebo obou

	Server			
Klient	**Specifické TLS 1.2 CipherSpec**	**ANY**	**ANY_ TLS12**	**ANY_TLS12_ OR_HIGHER**
Specifické TLS 1.2 CipherSpec	Připojení	Připojení	Připojení	Připojení
ANY	*Pravděpodobně nezdar*	Připojení	Připojení	Připojení
ANY_ TLS12	*Pravděpodobně nezdar*	Připojení	Připojení	Připojení
ANY_TLS12_ OR_HIGHER	*Pravděpodobně nezdar*	Připojení	Připojení	Připojení

Tabulka 79. Očekávané chování, je-li na straně klienta i serveru povoleno zabezpečení TLS 1.3

	Server						
Klient	**Specifické TLS 1.2 CipherSpec**	**Specifické TLS 1.3 CipherSpec**	**ANY**	**ANY_TLS 12**	**ANY_TLS 13**	**ANY_TLS12_ OR_VYŠŠÍ**	**ANY_TLS13_ OR_VYŠŠÍ**
Specifické TLS 1.2 CipherSpec	Připojení	**Selhání**	Připojení	Připojení	**Selhání**	Připojení	**Selhání**
Specifické TLS 1.3 CipherSpec	**Selhání**	Připojení	Připojení	**Selhání**	Připojení	Připojení	Připojení
ANY	**Selhání**	*Pravděpodobně nezdar*	Připojení	**Selhání**	Připojení	Připojení	Připojení
ANY_TLS12	*Pravděpodobně nezdar*	**Selhání**	Připojení	Připojení	**Selhání**	Připojení	**Selhání**
ANY_TLS13	**Selhání**	*Pravděpodobně nezdar*	Připojení	**Selhání**	Připojení	Připojení	Připojení

Tabulka 79. Očekávané chování, je-li na straně klienta i serveru povoleno zabezpečení TLS 1.3 (pokračování)							
	Server						
Klient	**Specifické TLS 1.2 CipherSpec**	**Specifické TLS 1.3 CipherSpec**	**ANY**	**ANY_TLS 12**	**ANY_TLS 13**	**ANY_TLS12_ OR_VYŠŠÍ**	**ANY_TLS13_ OR_VYŠŠÍ**
ANY_TLS12_ OR_HIGHER	**Selhání**	*Pravděpodobně nezdar*	Připojení	**Selhání**	Připojení	Připojení	Připojení
ANY_TLS13_ OR_HIGHER	**Selhání**	*Pravděpodobně nezdar*	Připojení	**Selhání**	Připojení	Připojení	Připojení

Související pojmy

"Digitální certifikáty a kompatibilita CipherSpec v produktu IBM MQ" na stránce 43
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 17
Kryptografické bezpečnostní protokoly musí souhlasit s algoritmem používaným zabezpečeným připojením. CipherSpecs a CipherSuites definují specifické kombinace algoritmů.

"Povolení CipherSpecs" na stránce 408
Povolte CipherSpec pomocí parametru **SSLCIPH** v příkazu **DEFINE CHANNEL** nebo **ALTER CHANNEL** MQSC.

Související úlohy

Migrace existujících konfigurací zabezpečení pro použití produktu ANY_TLS12_OR_HIGHER CipherSpec

Získání informací o CipherSpecs pomocí produktu IBM MQ Explorer

K zobrazení popisů CipherSpecsmůžete použít produkt IBM MQ Explorer .

Chcete-li získat informace o CipherSpecs v produktu "Povolení CipherSpecs" na stránce 408, 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 **Kanály**.
4. Klepněte pravým tlačítkem myši na kanál, se kterým chcete pracovat, a vyberte **Vlastnosti**.
5. Vyberte stránku vlastností **SSL** .
6. Vyberte ze seznamu CipherSpec , se kterou chcete pracovat. Popis se zobrazí v okně pod seznamem.

z/OS IBM i Alternativy ke specifikaci CipherSpecs

Pro platformy, ve kterých operační systém poskytuje podporu TLS, může váš systém podporovat nové specifikace CipherSpecs , které nejsou zahrnuty v produktu "Povolení CipherSpecs" na stránce 408.

Můžete uvést novou CipherSpec s parametrem SSLCIPH, ale hodnota, kterou zadáte, závisí na použité platformě. Ve všech případech musí specifikace odpovídat platnému protokolu TLS CipherSpec , který je platný a podporovaný verzí protokolu TLS, který systém spouští.

Poznámka: Tento oddíl se nevztahuje na systémy AIX, Linux, and Windows , protože CipherSpecs jsou dodávány s produktem IBM MQ , takže nové specifikace CipherSpecs nebudou po odeslání k dispozici.

IBM i IBM i

Dvouznakový řetězec reprezentující hexadecimální hodnotu.

Další informace o povolených hodnotách najdete v bodě tři v části Poznámky k použití Nastavit informace o znacích pro zabezpečenou relaci.

Upozornění: V **SSLCIPH**byste neměli uvádět hexadecimální hodnoty šifer, protože není zřejmé z hodnoty, která šifra bude použita, a výběr protokolu, který má být použit, je neurčitý. Použití hexadecimálních šifrovacích hodnot může vést k chybám neshody specifikace CipherSpec.

Pro uvedení hodnoty můžete použít buď příkaz **CHGMQMCHL** , nebo příkaz **CRTMQMCHL** , například:

```
CRTMQMCHL CHLNAME(' channel name ') SSLCIPH(' hexadecimal value ')
```

Pro nastavení parametru **SSLCIPH** můžete také použít příkaz MQSC **ALTER QMGR** .

z/OS **z/OS**

Four-znakový řetězec reprezentující hexadecimální hodnotu. Hexadecimální kódy odpovídají hodnotám definovaným v protokolu TLS.

Další informace naleznete v tématu Definice šifrovacích sad , kde je uveden seznam všech podporovaných specifikací šifer TLS 1.0, TLS 1.2a TLS 1.3 ve formátu 4místných hexadecimálních kódů.

Poznámka: Chcete-li použít slabé CipherSpecnebo CipherSpec náležící k zamítnutému protokolu, jako je zabezpečení SSL V3.0 nebo TLS 1.0, musíte v JCL inicializátoru kanálu zadat příslušnou kartu definice dat. Další informace viz “Zamítnuté specifikace CipherSpecs” na stránce 424.

Aspekty pro klastry IBM MQ

S klastry produktu IBM MQ je nejbezpečnější použít názvy CipherSpec v produktu “Povolení CipherSpecs” na stránce 408. Používáte-li alternativní specifikaci, uvědomte si, že specifikace nemusí být platná na jiných platformách. Další informace jsou uvedeny v tématu “protokol SSL/TLS” na stránce 470.

Určení CipherSpec pro IBM MQ MQI client

Pro specifikaci CipherSpec pro produkt IBM MQ MQI clientjsou k dispozici tři možnosti.

Jedná se o následující volby:

- Použití tabulky definic kanálů
- Použití pole SSLCipherSpec ve struktuře MQCD, v MQCD_VERSION_7 nebo vyšší, na volání MQCONNX.
- Použití Active Directory (na systémech Windows s podporou Active Directory)

Určení sady CipherSuite s IBM MQ classes for Java a IBM MQ classes for JMS

IBM MQ classes for Java a IBM MQ classes for JMS specifikujte CipherSuites jinak než u jiných platforem.

Další informace o určení sady CipherSuite s produktem IBM MQ classes for Javanaleznete v tématu Podpora zabezpečení TLS (Transport Layer Security) pro produkt Java .

Informace o určení sady CipherSuite s produktem IBM MQ classes for JMSnaleznete v tématu Použití zabezpečení TLS (Transport Layer Security) s produktem IBM MQ classes for JMS .

Určení CipherSpec pro IBM MQ.NET

Pro produkt IBM MQ.NET můžete určit volbu CipherSpec buď pomocí třídy MQEnvironment, nebo pomocí vlastnosti MQC.SSL_CIPHER_SPEC_PROPERTY v hašovací tabulce vlastností připojení.

Informace o určení CipherSpec pro nespravovaného klienta .NET naleznete v tématu Povolení zabezpečení TLS pro nespravovaný klient .NET .

Informace o specifikaci CipherSpec pro spravovaného klienta produktu .NET naleznete v tématu PodporaCipherSpec pro spravovaného klienta .NET .

z/OS Použití AT-TLS s IBM MQ for z/OS

Aplikace Transparent Transport Layer Security (AT-TLS) poskytuje podporu TLS pro aplikace z/OS , aniž by tyto aplikace musely implementovat podporu TLS, nebo dokonce být informovány o tom, že se TLS používá. AT-TLS je k dispozici pouze na z/OS.

AT-TLS lze použít se všemi verzemi produktu IBM MQ for z/OS.

Před použitím příkazu AT-TLS s produktem IBM MQ for z/OSse ujistěte, že jste se zapojili do produktu “Omezení” na stránce 436 .

Chcete-li použít Application Transparent Transport Layer Security , definujete příkazy zásad obsahující sadu pravidel, které používá server z/OS Communications Server k rozhodnutí, která připojení TCP/IP mají TLS transparentní povoleno.

Produkt IBM MQ for z/OS má svou vlastní implementaci TLS, která vyžaduje, aby kanály měly parametr SSLCIPH nakonfigurovaný s podporovanou specifikací CipherSpec.

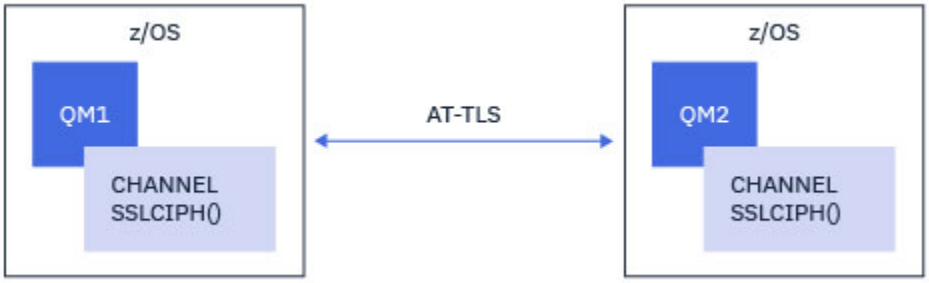
Při rozhodování o povolení zabezpečení TLS v kanálu může administrátor produktu IBM MQ rozhodnout o použití AT-TLS nebo IBM MQ TLS. Rozhodnutí se často provádí na základě toho, zda se AT-TLS používá pro jiný middleware, nebo z důvodu výkonu. Základní porovnání výkonu AT-TLS a IBM MQ TLS najdete v tématu MP16: Capacity Planning and Tuning for IBM MQ for z/OS.

Scénáře

Použití AT-TLS s produktem IBM MQ je podporováno v následujících scénářích:

Scénář 1

Mezi dvěma správci front produktu IBM MQ for z/OS , kde obě strany kanálu používají AT-TLS. To znamená, že ani kanál určuje atribut SSLCIPH. Tento přístup lze použít s libovolným kanálem zpráv.



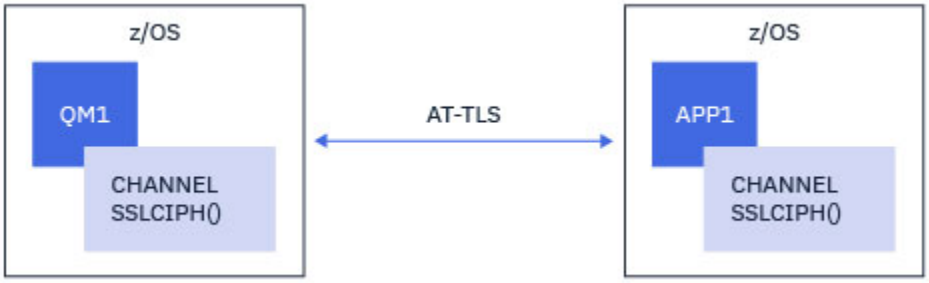
Implementace tohoto scénáře se skládá z definování dvou zásad AT-TLS, jedna pro každou stranu kanálu. Tyto zásady jsou stejné jako ty, které se používají buď se scénářem 3 , nebo Scénář 4.

Například, pokud byl kanál měněn pomocí jediné pojmenované CipherSpec pro použití AT-TLS, odchozí kanál bude používat zásadu z “Konfigurace AT-TLS v odchozím kanálu pro správce front IBM MQ for Multiplatforms s použitím jednoho názvu s názvem CipherSpec” na stránce 437 a příchozí kanál použije zásadu z “Konfigurace AT-TLS v příchozím kanálu ze správce front IBM MQ for Multiplatforms s použitím jediného názvu CipherSpec” na stránce 445.

Pokud byl kanál změněn z použití aliasu CipherSpec pro 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 441 a kanál příchozích požadavků použije zásadu z produktu “Konfigurace AT-TLS v příchozím kanálu ze správce front IBM MQ for Multiplatforms pomocí aliasu CipherSpec” na stránce 450.

Scénář 2

Mezi správcem front produktu IBM MQ for z/OS a klientskou aplikací IBM MQ Java spuštěnou v produktu z/OS , kde obě strany kanálu používají AT-TLS. To znamená, že ani kanál připojení serveru, ani kanál připojení klienta určuje atribut SSLCIPH.



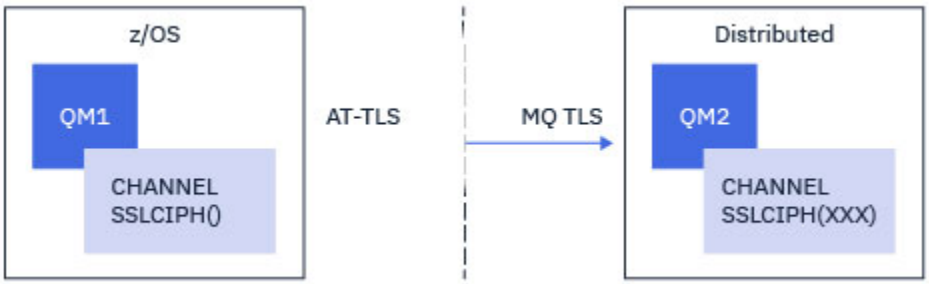
Implementace tohoto scénáře se skládá z definování dvou zásad AT-TLS, jedna pro každou stranu kanálu. Tyto zásady jsou stejné jako ty, které se používají buď se scénářem 3 , nebo Scénář 4.

Například, pokud byl kanál měněn z použití jediné pojmenované CipherSpec pro použití AT-TLS, kanál připojení klienta by použil 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 437 a kanál připojení serveru by tuto zásadu použil z produktu “Konfigurace AT-TLS v příchozím kanálu ze správce front IBM MQ for Multiplatforms s použitím jediného názvu CipherSpec” na stránce 445.

Pokud byl kanál měněn z použití aliasu CipherSpec pro 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 441 a kanál připojení serveru použije tuto zásadu z produktu “Konfigurace AT-TLS v příchozím kanálu ze správce front IBM MQ for Multiplatforms pomocí aliasu CipherSpec” na stránce 450.

Scénář 3

Mezi správcem front produktu IBM MQ for z/OS a správcem front spuštěnými v systému IBM MQ for Multiplatforms, kde správce front produktu IBM MQ for z/OS používá AT-TLS a správce front produktu IBM MQ for Multiplatforms používá IBM MQ TLS. Toto platí pro všechny jiné typy kanálů zpráv, kromě odesílatele klastru a příjemce klastru.

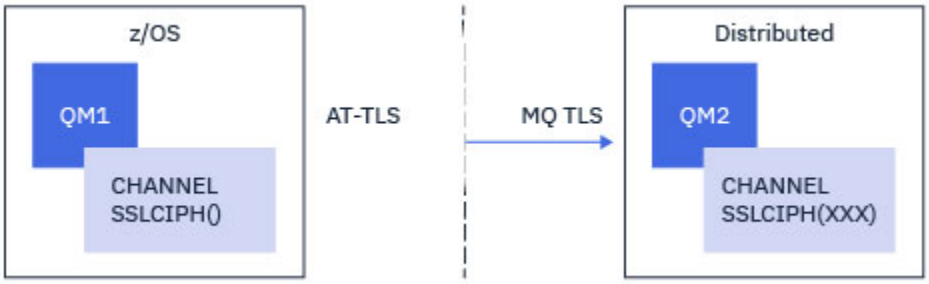


Příklad konfigurace typu AT-TLS pro odchozí kanály ze správce front produktu IBM MQ for z/OS se správcem front IBM MQ for Multiplatforms a “Konfigurace AT-TLS v příchozím kanálu ze správce front IBM MQ for Multiplatforms s použitím jediného názvu CipherSpec” na stránce 445 v případě příchozích kanálů ze správce front produktu IBM MQ for Multiplatforms do správce front IBM MQ for z/OS 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 437 .

Stejnou konfiguraci AT-TLS lze použít v případě, že jsou oba správci front v produktu z/OS, ale správce front na pravé straně nebyl konfigurován pro použití AT-TLS.

Scénář 4

Mezi správcem front produktu IBM MQ for z/OS a správcem front spuštěnými v systému IBM MQ for Multiplatforms, kde správce front produktu IBM MQ for z/OS používá AT-TLS a správce front produktu IBM MQ for Multiplatforms používá zabezpečení IBM MQ , je-li zadán atribut SSLCIPH s aliasem CipherSpec. Toto platí pro všechny jiné typy kanálů zpráv, kromě odesílatele klastru a příjemce klastru.



Příklad konfigurace typu AT-TLS pro odchozí kanály ze správce front produktu IBM MQ for z/OS se správcem front IBM MQ for Multiplatforms a “Konfigurace AT-TLS v příchozím kanálu ze správce front IBM MQ for Multiplatforms pomocí aliasu CipherSpec” na stránce 450a “Konfigurace AT-TLS v příchozím kanálu ze správce front IBM MQ for Multiplatforms pomocí aliasu CipherSpec” na stránce 450 v případě příchozích kanálů ze správce front produktu IBM MQ for Multiplatforms do správce front produktu IBM MQ for z/OS naleznete v tématu “Konfigurace AT-TLS v odchozím kanálu pro správce front IBM MQ for Multiplatforms s použitím aliasu CipherSpecs” na stránce 441 .

Stejnou konfiguraci AT-TLS lze použít v případě, že jsou oba správci front v produktu z/OS, ale správce front na pravé straně nebyl konfigurován pro použití AT-TLS.

Scénář 5

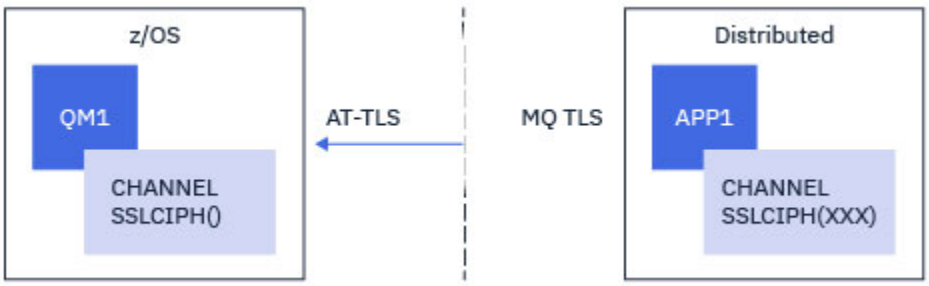
Mezi správcem front produktu IBM MQ for z/OS a klientskou aplikací spuštěnou v produktu IBM MQ for Multiplatforms, kde správce front produktu IBM MQ for z/OS používá protokol AT-TLS a klientská aplikace používá produkt IBM MQ TLS, určuje atribut SSLCIPH s jedním názvem s názvem CipherSpec.

Tento scénář vyžaduje jednu zásadu AT-TLS, která splňuje stejné požadavky jako ty, které používají příchozí kanál zpráv; viz “Konfigurace AT-TLS v příchozím kanálu ze správce front IBM MQ for Multiplatforms s použitím jediného názvu CipherSpec” na stránce 445.

Stejnou konfiguraci typu AT-TLS lze použít, je-li klientská aplikace aplikací Java a je spuštěna také v systému z/OS, ale nebyla konfigurována pro použití AT-TLS.

Scénář 6

Mezi správcem front produktu IBM MQ for z/OS a klientskou aplikací spuštěnou v produktu IBM MQ for Multiplatforms, kde správce front produktu IBM MQ for z/OS používá AT-TLS a klientská aplikace používá produkt IBM MQ TLS tak, že určuje atribut SSLCIPH s aliasem CipherSpec.



Tento scénář vyžaduje jednu zásadu AT-TLS, která splňuje stejné požadavky jako ty, které používají příchozí kanál zpráv; viz “Konfigurace AT-TLS v příchozím kanálu ze správce front IBM MQ for Multiplatforms pomocí aliasu CipherSpec” na stránce 450.

Stejnou konfiguraci typu AT-TLS lze použít, je-li klientská aplikace aplikací Java a je spuštěna také v systému z/OS, ale nebyla konfigurována pro použití AT-TLS.

Omezení

IBM MQ for z/OS není AT-TLS aware, proto existuje několik omezení, která platí pro předchozí scénáře:

- AT-TLS v kombinaci s produktem IBM MQ TLS nepracuje s kanály odesílatele klastru a přijímačů klastru.
- Správci front produktu IBM MQ for z/OS nejsou informováni o tom, že používají AT-TLS a nepřijímají žádné informace o certifikátu od svého partnerského správce front nebo klienta. Následující atributy proto nemají žádný vliv na stranu z/OS kanálu pomocí AT-TLS:
  - Atributy kanálu SSLCAUTH a kanálu SSLPEER
  - Atribut správce front SSLRKEYC
  - Atributy SSLPEERMAP pro pravidla CHLAUTH
- Použití nového vyjednávání tajného klíče TLS vyžaduje, aby obě strany kanálu používaly IBM MQ TLS. Proto by správce front produktu IBM MQ for Multiplatforms nebo klient neměl mít povoleno opakované domlouvání TLS, pokud se připojuje ke správci front produktu IBM MQ for z/OS pomocí AT-TLS.

  Chcete-li zakázat opětovné sjednání 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 454.

Konfigurační příkazy AT-TLS

AT-TLS je konfigurováno pomocí sady příkazů. Hodnoty použité ve scénářích dokumentovaných v tomto tématu jsou:

TTLSRule
Určuje sadu kritérií pro porovnání připojení TCP/IP ke konfiguraci TLS. To se dále odkazuje na jiné typy příkazů.

TTLSGroupAction
Uvádí, zda je odkaz `TTLSRule` povolen nebo ne.

TTLSEnvironmentAction
Určuje podrobnou konfiguraci pro odkazující produkt `TTLSRule` a odkazuje na počet dalších příkazů.

TTLSKeyringParms
Odkazuje na soubor svazku klíčů, který má být použit pro AT-TLS.

TTLSCipherParms
Definuje sady šifer, které mají být použity.

TTLSEnvironmentAdvancedParametry
Definuje, které protokoly TLS nebo SSL jsou povoleny.

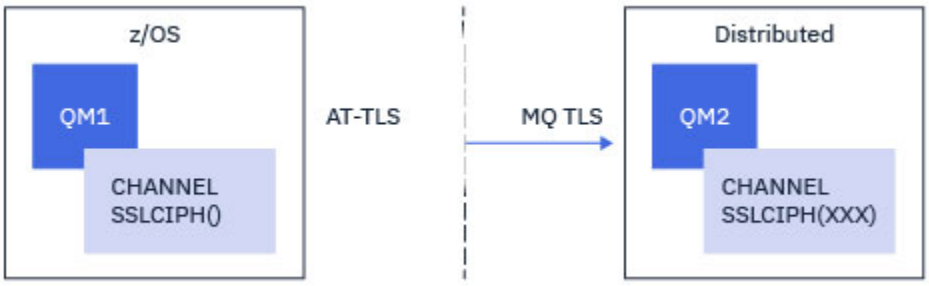
Upozornění: Jsou zde další příkazy zásad AT-TLS s AT-TLS, které zde nejsou dokumentovány a lze je použít s IBM MQ v závislosti na potřebě. Produkt IBM MQ však byl testován pouze se zásadami popsanými v tomto tématu.

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 441 .

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.



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.

Upozornění: Protokol TLS 1.3 lze použít pouze v produktu z/OS verze 2.4 nebo vyšší.

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 není z/OS . Tento svazek klíčů lze definovat stejným způsobem jako svazek klíčů používaný inicializátorem kanálu; viz “Konfigurace systému z/OS pro použití TLS” na stránce 250.

```
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 80. 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

Tabulka 80. CipherSpecs na z/OS z IBM MQ for z/OS 9.2.0 (pokračování)			
CipherSpec	**Protokol**	**Hexadecimální kód**	**Standardně povoleno**
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
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

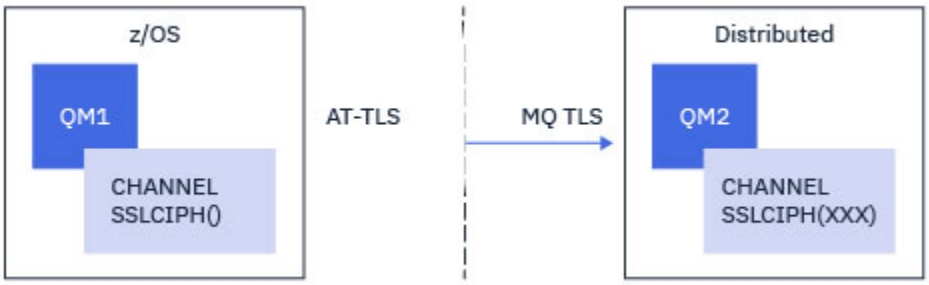
Jakmile je kanál spuštěn, bude používat kombinaci AT-TLS a IBM MQ TLS.

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.

Upozornění: Protokol TLS 1.3 lze použít pouze v produktu z/OS verze 2.4 nebo vyšší.

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 250.

```
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 81. 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
TRIPLE_DES_SHA_US	SSL v3	000A	Ne
RC4_SHA_US	SSL v3	0005	Ne
RC4_MD5_US	SSL v3	0004	Ne

Tabulka 81. CipherSpecs na z/OS z IBM MQ for z/OS 9.2.0 (pokračování)			
CipherSpec	**Protokol**	**Hexadecimální kód**	**Standardně povoleno**
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 nastavením aliasu CipherSpec” na stránce 429 .

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.

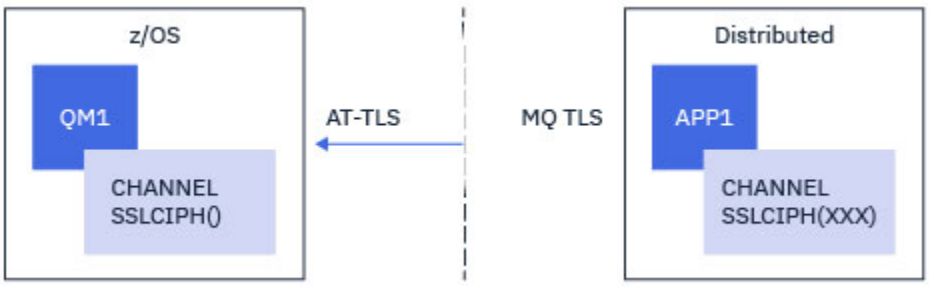
Upozornění: Předchozí příkazy AT-TLS jsou pouze minimální konfigurací. Existují další příkazy zásad AT-TLS s AT-TLS, které zde nejsou dokumentovány, a v závislosti na potřebě je lze použít s produktem IBM MQ . Produkt IBM MQ však byl testován pouze s popsanými zásadami.

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 450 .

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.

Upozornění: Protokol TLS 1.3 lze použít pouze v produktu z/OS verze 2.4 nebo vyšší.

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 250.

```
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 82. 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

Tabulka 82. CipherSpecs na z/OS z IBM MQ for z/OS 9.2.0 (pokračování)			
CipherSpec	**Protokol**	**Hexadecimální kód**	**Standardně povoleno**
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

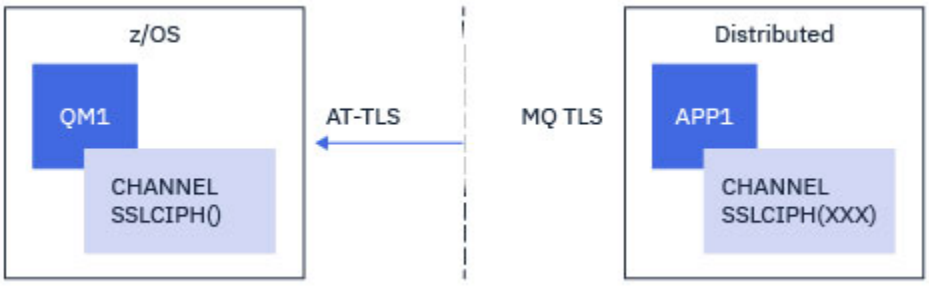
Jakmile je kanál spuštěn, bude používat kombinaci AT-TLS a IBM MQ TLS.

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.

Upozornění: Protokol TLS 1.3 lze použít pouze v produktu z/OS verze 2.4 nebo vyšší.

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 250.

```
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 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

Tabulka 83. 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 nastavením aliasu CipherSpec” na stránce 429 .

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.

V systému IBM ipoužijte parametr **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 Počet KeyResetve struktuře MQSCO ve volání MQCONNX.
2. Pomocí proměnné prostředí MQSSLRESET
3. Nastavením atributu Počet SSLKeyResetv konfiguračním souboru klienta MQI.

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.

Úplné podrobnosti o struktuře MQSCO naleznete v tématu KeyResetPočet (MQLONG). Úplné podrobnosti o příkazu MQSSLRESET viz MQSSLRESET. Další informace o použití TLS v konfiguračním souboru klienta viz Sekce SSL konfiguračního souboru klienta.

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 nespravované klienty systému .NET celočíselná vlastnost SSLKeyResetPočet označuje počet nešifrovaných bajtů odeslaných a přijatých v rámci konverzace TLS před opětovným vyjednáním tajného klíče.

Chcete-li získat informace o použití vlastností objektu v souboru IBM MQ classes for .NET, prohlédněte si téma 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 počet SSLKeyReset. 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
ZOBRAZENÍ SPRÁVCE FRONT
Změna správce front zpráv (CHGMQM)
Zobrazení správce front zpráv (DSPMQM)

Implementace utajení v uživatelských ukončovacích programech

Implementace utajení v uživatelských procedurách zabezpečení

Uživatelské procedury zabezpečení mohou hrát roli ve službě důvěrnosti tím, že generují a distribuují symetrický klíč pro šifrování a dešifrování dat, která proudí na kanál. Běžnou technikou pro to je využití technologie PKI.

Jedna uživatelská procedura zabezpečení vygeneruje náhodnou datovou hodnotu, zašifruje ji pomocí veřejného klíče správce front nebo uživatele, který zástupce pro zabezpečení partnera reprezentuje, a odešle zašifrovaná data svému partnerovi do zprávy zabezpečení. Partner pro zabezpečení ochrany dat dešifruje náhodná hodnotu dat se soukromým klíčem správce front nebo uživatele, který reprezentuje. Každá uživatelská procedura zabezpečení může nyní použít hodnotu náhodných dat k odvozování symetrického klíče nezávisle na sobě pomocí algoritmu, který je znám oběma z nich. Případně mohou použít hodnotu náhodných dat jako klíč.

Pokud první bezpečnostní procedura neověřila svého partnera do této doby, další zpráva zabezpečení odeslaná partnerem může obsahovat očekávanou hodnotu šifrovanou pomocí symetrického klíče. První uživatelská procedura zabezpečení může nyní ověřit svého partnera kontrolou, zda byla uživatelská procedura zabezpečení partnera schopna správně zašifrovat očekávanou hodnotu.

Uživatelské procedury zabezpečení mohou také využít této příležitosti k tomu, aby se shodly na algoritmu pro šifrování a dešifrování dat, která proudí na kanálu, je-li k dispozici více než jeden algoritmus pro použití.

Implementace utajení ve výstupních procedurách zprávy

Ukončení zprávy na odesílajícím konci kanálu může zašifrovat data aplikace ve zprávě a další ukončení zprávy na přijímajícím konci kanálu může data dešifrovat. Z důvodu výkonu se za tímto účelem obvykle používá algoritmus symetrického klíče. Další informace o tom, jak lze symetrický klíč generovat a distribuovat, viz “Implementace utajení v uživatelských ukončovacích programech” na stránce 456.

Záhlaví ve zprávě, jako je záhlaví přenosové fronty, MQXQH, která obsahuje vložený deskriptor zprávy, nesmí být šifrována uživatelskou procedurou pro zprávy. Důvodem je to, že k převodu dat záhlaví zpráv dochází buď po zavolání uživatelské procedury zprávy na odesílající straně, nebo před zavoláním ukončení zprávy na přijímajícím konci. Pokud jsou záhlaví šifrována, převod dat se nezdaří a kanál se zastaví.

Implementace utajení v uživatelských procedurách odesílání a příjmu

Uživatelské procedury pro odeslání a přijetí lze použít k šifrování a dešifrování dat, která proudí na kanál. Pro poskytnutí této služby jsou vhodnější než zprávy pro poskytování této služby z následujících důvodů:

- Na kanálu zpráv mohou být záhlaví zpráv zašifrována a data aplikace ve zprávách.
- Uživatelské procedury pro odesílání a příjem lze použít na kanálech MQI a také v kanálech zpráv. Parametry v voláních MQI mohou obsahovat citlivá data aplikací, která je třeba chránit při průběžích kanálu MQI. Proto můžete používat stejné uživatelské procedury pro odesílání a příjem na obou druzích kanálů.

Implementace důvěrnosti ve výstupu rozhraní API a ukončení přeletu rozhraní API

Data aplikace ve zprávě lze šifrovat pomocí rozhraní API nebo opuštění rozhraní API, když je zpráva vložena do odesílající aplikace a dešifrována druhou uživatelskou procedurou, když je zpráva načtena přijímající aplikací. Z výkonnostních důvodů se pro tento účel obvykle používá algoritmus symetrického klíče. Avšak, na úrovni aplikace, kde mnoho uživatelů může odesílat zprávy navzájem, problém spočívá v tom, jak zajistit, aby pouze zamýšlený příjemce zprávy byl schopen dešifrovat zprávu. Jedním řešením je použití odlišného symetrického klíče pro každou dvojici uživatelů, kteří mezi sebou posílají zprávy. Toto řešení však může být obtížné a časově náročné, zejména v případě, že uživatelé patří k různým organizacím. 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 překřížení rozhraní API vygeneruje náhodný symetrický klíč a použije klíč k zašifrování dat aplikace ve zprávě. Uživatelská procedura zašifruje symetrický klíč s veřejným klíčem určeného příjemce. Poté nahradí data aplikace ve zprávě s šifrovanými daty aplikace a zašifrovaným symetrickým klíčem. Tímto způsobem může pouze určený příjemce dešifrovat symetrický klíč, a tím i data aplikace. Pokud má šifrovaná zpráva více možných zamýšlených zásobníků, může ukončení zašifrovat kopii symetrického klíče pro každý zamýšlený zásobník.

Pokud jsou pro použití k dispozici různé algoritmy pro šifrování a dešifrování dat aplikace, může uživatelská procedura obsahovat název algoritmu, který používá.

z/OS V 9.2.0 Utajení dat ve zbytku IBM MQ for z/OS s šifrováním datové sady

IBM MQ for z/OS může ztvrdnout data zákazníků a konfiguračních dat zápisem dat do aktivních datových sad protokolů, datových sad protokolu archivace, sad stránek, zaváděcí datové sady (BSDS) a sdílené datové sady zpráv (SMDS).

z/OS poskytuje efektivní šifrování datových sad na základě zásad. Produkt IBM MQ for z/OS podporuje šifrování dat produktu z/OS pro:

- Aktivní datové sady žurnálu; viz poznámka “1” na stránce 458
- Archivní datové sady protokolu; viz poznámka “2” na stránce 458
- Sady stránek; viz poznámka “1” na stránce 458
- BSDS; viz poznámka “2” na stránce 458

- datové sady CSQINP*; viz poznámka “2” na stránce 458
- V 9.2.0 SMDS; viz poznámka “1” na stránce 458

Tím je zajištěna důvěrnost dat ve zbytku správce front v systému z/OS .

Notes:

1. V 9.2.0 Z IBM MQ for z/OS 9.2.0, z/OS šifrování datové sady pro aktivní protokoly. jsou podporovány sady stránek a SMDS.
2. Šifrování datové sady pro protokoly archivace, BSDS a datové sady CSQINP* jsou podporovány ve všech verzích produktu IBM MQ for z/OS.
3. IBM MQ Advanced Message Security poskytuje alternativní mechanizmus ochrany dat v klidu. Kromě AMS také chrání data v paměti a v letu.

Další informace o šifrování datové sady produktu z/OS naleznete v tématu Použití vylepšení šifrování datové sady operačního systému z/OS .

Konfigurace šifrování datové sady produktu z/OS se nachází mimo ovládací prvek produktu IBM MQ for z/OS. Nastavení šifrování se projeví po vytvoření datové sady.

To znamená, že všechny existující datové sady musí být znovu vytvořeny, aby bylo možné použít novou zásadu šifrování datové sady.

Produkt IBM MQ for z/OS může být spuštěn se směsí šifrovaných a nezašifrovaných datových sad, ale standardní konfigurace by šifrovala všechny použité datové sady nebo žádné.

z/OS V 9.2.0 Přehled kroků k zašifrování datové sady IBM MQ for z/OS

Způsob šifrování datové sady produktu IBM MQ for z/OS .

Než začnete

Musíte se ujistit, že jste ve svém podniku správně nakonfigurovali šifrování dat produktu z/OS ve vašem podniku. Nastavujete-li šifrování datové sady ve skupině sdílení front, je třeba pro sdílení dat nakonfigurovat šifrování datové sady produktu z/OS .

Poznámka: Zašifrovaná datová sada z/OS musí být datová sada rozšířeného formátu.

Postup

1. Nastavte šifrovací klíč a `key-label` v RACF pro použití k zašifrování datové sady.
2. Vytvořte profil pro prostor `key-label` ve třídě RACF CSFKEYS.
3. Udělte uživateli READ přístup k ID uživatele správce front a všechny ostatní ID uživatelů, kteří potřebují přístup k šifrovaným datům.

   To může zahrnovat ID uživatelů, která se používají ke spuštění obslužných programů tisku pro datovou sadu. Například uživatel, který spouští operaci CSQUTIL SCOPY, by měl dešifrovat příslušnou sadu stránek.
4. Přidružte šifrování `key-label` k názvu datové sady.

   To můžete provést pomocí třídy dat SMS nebo segmentu RACF DFP, pro název datové sady nebo kvalifikátor vyšší úrovně.

   `key-label` můžete také přidružit k datové sadě, když je datová sada přidělena.
5. Přejmenujte existující datovou sadu pomocí příkazu IDCAMS ALTER.
6. Znovu přidělte datovou sadu s příslušnými atributy.
7. Zkopírujte obsah přejmenované datové sady na novou datovou sadu pomocí IDCAMS REPRO.

   Data jsou šifrována pomocí akce kopírování do datové sady.
8. Opakujte kroky “4” na stránce 458 až “6” na stránce 458 pro všechny ostatní datové sady, které je třeba zašifrovat.

z/OS V 9.2.0 Příklad, jak šifrovat aktivní protokoly správce front

Následující témata vás provedou procesem povolování šifrování datové sady v existujících aktivních protokolech.

Poznámka: Proces pro další datové sady je podobný jako u aktivních protokolů.

V tomto příkladu platí následující:

- Správce front CSQ1 je spuštěn pod uživatelem QMCSQ1a má aktivní datové sady protokolu CSQ1.LOGS.LOGCOPY1.DS001, CSQ1.LOGS.LOGCOPY1.DS002, atd.
- Hardwarové a softwarové prostředí je schopné používat šifrování datové sady produktu z/OS .
- RACF se používá jako SAF
- Správce front byl zastaven.

Proveďte tento postup v následujícím pořadí:

1. “Konfigurace šifrovacího klíče datové sady pro správce front” na stránce 459
2. “Konfigurace šifrování datové sady pro datové sady protokolu” na stránce 460

z/OS V 9.2.0 Konfigurace šifrovacího klíče datové sady pro správce front

Způsob konfigurace šifrovacího klíče datové sady pro správce front.

Informace o této úloze

Tato úloha je nezbytným předpokladem pro produkt “Konfigurace šifrování datové sady pro datové sady protokolu” na stránce 460.

Postup

1. Nastavte klíč bitového šifrování AES-256 s popiskem, například CSQ1DSKY, pomocí obslužného programu z/OS key generator utility program (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. Povolit správci front použít šifrovací klíč zadáním příkazu QMCSQ1 READ k profilu, zadáním následujícího příkazu:

   ```
   PERMIT CSQ1DSKY CLASS(CSFKEYS) ID(QMCSQ1) ACCESS(READ)
   ```

   Dejte stejnému přístupu k administrativnímu uživateli, který potřebuje číst nebo zapisovat šifrovanou datovou sadu.
5. Aktualizujte třídu CSFKEYS zadáním následujícího příkazu.

   ```
   SETROPTS RACLIST(CSFKEYS) REFRESH
   ```

Jak pokračovat dále

Nakonfigurovat šifrování datové sady pro datové sady, jak je popsáno v tématu “Konfigurace šifrování datové sady pro datové sady protokolu” na stránce 460

z/OS V 9.2.0 Konfigurace šifrování datové sady pro datové sady protokolu

Způsob konfigurace šifrování v datových sadách protokolu.

Než začnete

Ujistěte se, že jste přečetli:

Přehled kroků pro šifrování datové sady produktu IBM MQ for z/OSa provádění procedury v “Konfigurace šifrovacího klíče datové sady pro správce front” na stránce 459

Informace o této úloze

Tato metoda používá segment DFP generického profilu RACF , takže můžete použít šifrovací klíč pro všechny nové datové sady, které se shodují s profilem.

Alternativně můžete nakonfigurovat a použít třídu dat SMS nebo popisek klíče lze zadat přímo při alokaci datové sady.

Jak již bylo dříve popsáno, v tomto příkladu je správce front CSQ1 spuštěn pod uživatelem QMCSQ1a má aktivní datové sady protokolu CSQ1.LOGS.LOGCOPY1.DS001, CSQ1.LOGS.LOGCOPY1.DS002a tak dále.

Postup

1. Pokud tento generický profil neexistuje, vytvořte jej zadáním následujícího příkazu:

   ```
   ADDSD 'CSQ1.LOGS.*' UACC(NONE)
   ```

2. Povolte přístup uživatele správce front k profilu tím, že zadáte tento příkaz:

   ```
   PERMIT 'CSQ1.LOGS.*' ID(QMCSQ1) ACCESS(ALTER)
   ```

   Také povolte odpovídající přístup potřebný pro všechny administrativní uživatele.

3. Přidejte segment DFP se jmenovkou šifrovacího klíče vyvoláním 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 profily generických datových sad 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) Přejmenujte datovou sadu na backup

   ```
   //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) Znovu definujte datovou sadu.

   Nová datová sada bude zašifrována kvůli profilu RACF.

Poznámka: Nahraďte + + EXTDCLASS + + s 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 zašifruje 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 460 pro všechny aktivní datové sady protokolů.

Je povinný pouze jeden šifrovací klíč a všechny datové sady mohou být přidruženy ke stejnému označení klíče.

Restartujte správce front CSQ1. Použijte výstup z příkazu DISPLAY LOG k ověření, že datové sady protokolu byly šifrovány.

z/OS V 9.2.0 Aspekty šifrování datové sady produktu z/OS ve skupině sdílení front

Každý správce front v rámci skupiny sdílení front (QSG) musí být schopen číst protokoly, BSDSa sdílené datové sady zpráv (SMDS) všech ostatních správců front v QSG.

To znamená, že každý systém, na kterém může být spuštěn člen skupiny QSG, musí splňovat požadavky na šifrování datové sady produktu z/OS a všechny klíčové štítky a šifrovací klíče použité k ochraně datových sad pro každého správce front v QSG, musí být dostupné na každém systému.

Správce front před produktem IBM MQ for z/OS 9.1.4 nemůže přistupovat k šifrované datové sadě aktivního žurnálu.

Správce front starší než IBM MQ for z/OS 9.1.5 nemůže přistupovat k zašifrované SMDS.

Před provedením šifrování datové sady produktu z/OS byste měli migrovat všechny správce front v rámci skupiny sdílení front na alespoň IBM MQ for z/OS 9.1.5.

Pokud je správce front ve skupině QSG spuštěn s libovolnou šifrovanou aktivní datovou sadou žurnálu a všechny ostatní správce front v QSG byly spuštěny, ale nebyly naposledy spuštěny s verzí produktu IBM MQ for z/OS , která podporuje šifrované aktivní protokoly, správce front s šifrovaným aktivním protokolem se ukončí nestandardně s kódem abend 5C6-00F50033.

QSG můžete převést na použití šifrovaných aktivních protokolů a SMDS bez úplného výpadku, tím, že:

1. Přemístění jednotlivých správců front na alespoň IBM MQ for z/OS 9.1.5 postupně.
2. Převod aktivních protokolů na šifrované datové sady pro jednotlivé správce front postupně. To vyžaduje, aby byl správce front vypnut a poté restartován.

Současně je pravděpodobné, že sady stránek a archivační protokoly budou povoleny i pro zašifrované datové sady, ale to neovlivní migraci QSG.

Procedura pro převod každé datové sady je popsána v tématu "Příklad, jak šifrovat aktivní protokoly správce front" na stránce 459 .

3. Převod sady SMDS do šifrovaných datových sad pro každou jednotlivou strukturu prostředku Coupling Facility, a to následujícím způsobem:
   a. Vydáním příkazu RESET SMDS (*) ACCESS (DISABLED) CFSTRUCT (název-struktury) pozastavte přístup správce front k SMDS.

      Všimněte si, že během této doby jsou data na sdílených frontách přidružených k SMDS dočasně nedostupná.
   b. Převod každé datové sady, která tvoří sadu SMDS do šifrovaných datových sad, pomocí procedury popsané v tématu "Příklad, jak šifrovat aktivní protokoly správce front" na stránce 459.
   c. Zadáním příkazu RESET SMDS (*) ACCESS (ENABLED) CFSTRUCT (structure-name) obnovte přístup správce front k SMDS.

Upozornění: Správce front byste měli před převedením protokolů ukončit čistě a v průběhu převodu nemusí být možné provést zotavení struktury prostředku Coupling Facility, protože aktivní datové sady žurnálu budou dočasně nedostupné.

z/OS V 9.2.0 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 462.

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 464 .

Odebrání šifrování datové sady z datové sady

Tento příklad popisuje, jak odebrat šifrování datové sady z datové sady protokolu CSQ1.LOGS.LOGCOPY1.DS001. Pro sady stránek V 9.2.0 SMDS a můžete použít ekvivalentní proces.

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 datových sad, pak všechny datové sady aktivních protokolů a SMDS všech správců front v rámci skupiny sdílení front musí mít odebrané zásady šifrování datových sad 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 462.

   Pokud má být správce front zpětně migrován, jeho sada stránek by měla být v tuto chvíli také dešifrována. Poté restartujte správce front.

2. V 9.2.0 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 462 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 462 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

Datová sada	Chyba, pokud správce front nepodporuje šifrování datové sady z/OS
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
V 9.2.0 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 ukončovacího programu k poskytování zpráv kódů digest 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. Pokud používáte produkt IBM MQ Advanced Message Service (AMS), můžete uvést integritu pro jedinečnou zprávu.

Implementace integrity dat ve výstupních procedurách zprávy

Zpráva může být digitálně podepsána ukončením zprávy na odesílajícím konci kanálu. Digitální podpis lze poté zkontrolovat uživatelskou procedurou na přijímajícím konci kanálu a zjistit, zda byla zpráva záměrně upravena.

Určitá ochrana může být poskytnuta použitím kódu digest zprávy místo digitálního podpisu. Kód digest zprávy může být účinný proti náhodnému nebo nevybíravému falšování, ale nezabrání tomu, aby byl informovanější jednotlivec měněn nebo nahrazován zprávou a generování zcela nového kódu digest pro tuto zprávu. To platí zejména v případě, že algoritmus používaný ke generování kódu digest zprávy je dobře známý.

Implementace integrity dat v uživatelských procedurách odesílání a příjmu

Na kanálu zpráv jsou uživatelské procedury pro poskytování této služby vhodnější, protože uživatelská procedura pro zprávy má přístup k celé zprávě. Na kanálu MQI mohou parametry volání MQI obsahovat data aplikace, která je třeba chránit, a tuto ochranu může poskytnout pouze odeslání a přijetí uživatelských procedur.

Implementace integrity dat v uživatelské proceduře rozhraní API nebo ukončení přeletu rozhraní API

Zprávu lze digitálně podepsat pomocí rozhraní API nebo předání rozhraní API, když je zpráva vložena odesílající aplikací. Digitální podpis pak může být zkontrolován druhou uživatelskou procedurou, když je zpráva načtena přijímající aplikací za účelem zjištění, zda byla zpráva úmyslně upravena.

Určitá ochrana může být poskytnuta použitím kódu digest zprávy místo digitálního podpisu. Kód digest zprávy může být účinný proti náhodnému nebo nevybíravému falšování, ale nezabrání tomu, aby byl informovanější jednotlivec měněn nebo nahrazován zprávou a generování zcela nového kódu digest pro tuto zprávu. 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 408 .

Související úlohy

Připojení dvou správců front pomocí protokolu TLS

Bezpečná připojení klienta ke správci front

Auditování

Můžete zkontrolovat narušení zabezpečení nebo pokusy o narušení pomocí zpráv událostí. Zabezpečení vašeho systému můžete také zkontrolovat pomocí 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 zprávami o událostech 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.

Uchování zabezpečených klastrů

Autorizujte nebo zabraňte správcům front připojujících se ke klastrům nebo vkládání zpráv do front klastru. Vynuťte, aby správce front opustil klastr. Při konfiguraci TLS pro klastry je třeba vzít v úvahu některé další aspekty.

Zastavení neautorizovaných správců front při odesílání zpráv

Zabraňte neautorizovaným správcům front odesílat zprávy do svého správce front pomocí uživatelské procedury zabezpečení kanálu.

Než začnete

Klastrování nemá žádný vliv na způsob, jakým zabezpečení ukončí práci. Přístup ke správci front lze omezit stejným způsobem jako v distribuovaném prostředí s frontami.

Informace o této úloze

Zabránit vybraným správcům front v odesílání zpráv do správce front:

Postup

1. Definujte uživatelský program zabezpečení kanálu na definici kanálu CLUSRCVR .
2. Napište program, který autentizuje správce front, který se pokouší odeslat zprávy na kanál příjemce klastru a odpírá jim přístup, pokud k nim nejsou autorizováni.

Jak pokračovat dále

Ukončovací programy zabezpečení kanálu jsou volány při inicializaci a ukončení agenta MCA.

Zastavení neautorizovaných správců front při vkládání zpráv do front

Použijte atribut autority vložení kanálu na přijímacím kanálu klastru, abyste zastavili neautorizované správce front, které umisťují zprávy do vašich front. Autorizujte vzdáleného správce front tím, že zkontrolujete ID uživatele ve zprávě pomocí produktu RACF v systému z/OSnebo na OAM na jiných platformách.

Informace o této úloze

K řízení přístupu k frontám slouží bezpečnostní zařízení platformy a mechanizmus řízení přístupu v produktu IBM MQ .

Postup

1. Chcete-li zabránit určitým správcům front ve vkládání zpráv do fronty, použijte nástroje zabezpečení, které jsou k dispozici na vaší platformě.

   Příklad:

- RACF nebo další externí správci zabezpečení v systému IBM MQ for z/OS
- Správce oprávnění k objektu (OAM) na jiných platformách.

2. Použijte příkaz put, PUTAUT, atribut na definici kanálu CLUSRCVR .

   Atribut PUTAUT vám umožňuje uvést, jaké 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 použití ID uživatele přijatého ze sítě a odvozeného od uživatele MCAUSER.

   CTX
   Použijte ID uživatele v kontextových informacích přidružených ke zprávě. V systému z/OS se kontrola může týkat buď použití ID uživatele přijatého ze sítě, nebo odvozeného od uživatele MCAUSER, nebo obou. Tuto volbu použijte, je-li odkaz důvěryhodný a ověřený.

   ONLYMCA (pouze z/OS)
   Co se týká DEF, ale žádné ID uživatele přijaté ze sítě se nepoužívá. Tuto volbu použijte v případě, že odkaz není důvěryhodný. Chcete povolit pouze specifickou sadu akcí na ní, které jsou definovány pro MCAUSER.

   ALTMCA (pouze z/OS)
   Co se týče CTX, ale žádné ID uživatele přijaté ze sítě se nepoužije.

Autorizace vkládání zpráv ve vzdálených frontách klastru

V produktu z/OS nastavte autorizaci pro vložení do fronty klastru pomocí produktu RACF. Na jiných platformách autorizujte přístup pro připojení ke správcům front a k jejich vložení 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 konfigurovali atribut **ClusterQueueAccessControl** v souboru qm.ini na hodnotu *RQMName*, jak je popsáno v tématu Sekce zabezpečení , a restartováním správce front.

Procedura

- Pro z/OSzadejte následující příkazy:

```
RDEFINE MQQUEUE QMgrName.QUEUE. QueueName UACC(NONE)
PERMIT QMgrName.QUEUE. QueueName CLASS(MQADMIN) ID(GroupName) ACCESS(UPDATE)
```

- Pro systémy 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 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 určené fronty klastru a žádné další 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, ke které má být udělen přístup.

QueueName
Název fronty nebo generický profil, pro který mají být změněna autorizace.

Jak pokračovat dále

Uvedete-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 vkládání zpráv do vzdálené fronty klastru" na stránce 386.

Související pojmy
Sekce zabezpečení v souboru qm.ini

Zabránění připojování správců front ke klastru

Pokud se k klastru připojí škodící správce front, je obtížné zabránit tomu, aby přijímala zprávy, které nechcete přijímat.

Postup

Chcete-li zajistit, aby se ke klastru připojili pouze určité autorizovaní správci front, máte na výběr ze tří technik:

- Pomocí záznamů ověření kanálu můžete zablokovat připojení ke kanálu klastru na základě: vzdálené adresy IP, názvu vzdáleného správce front nebo rozlišujícího názvu TLS poskytnutého vzdáleným systémem.
- Napište výstupní program, který zabrání neoprávněným správcům front zapisovat do `SYSTEM.CLUSTER.COMMAND.QUEUE`. Neomezujte přístup k produktu `SYSTEM.CLUSTER.COMMAND.QUEUE` tak, aby k němu mohl zapisovat žádný správce front, nebo byste zabránili libovolnému správci front v připojení ke klastru.
- Uživatelský program zabezpečení v definici kanálu produktu `CLUSRCVR` .

Uživatelské procedury zabezpečení na kanálech klastru

Další aspekty použití uživatelských procedur zabezpečení na kanálech klastru.

Informace o této úloze

Je-li odesílací kanál 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 se přepíše novými atributy, včetně atributu `SecurityExit` .

Postup

1. Je třeba definovat uživatelskou proceduru zabezpečení na straně odesílatele klastru i na konci kanálu příjemce klastru.

   Počáteční připojení musí být provedeno pomocí handshake handshake, i když je jméno uživatelské procedury zabezpečení posláno z definice příjemce klastru.
2. Ověřte `PartnerName` ve struktuře `MQCXP` v uživatelské proceduře pro zabezpečení zprávy.

   Uživatelská procedura musí umožňovat spuštění kanálu pouze v případě, že je správce front partnera autorizován.
3. Navrhněte proceduru zabezpečení v definici příjemce klastru, která má být iniciován příjemcem.

4. Pokud ji navrhujete jako odesilatele, může neautorizovaný správce front bez ukončení zabezpečení vstoupit do klastru, protože se neprovedou žádné kontroly zabezpečení.

   Ne, dokud nebude kanál zastaven a restartován může být název SCYEXIT odeslán z definice příjemce klastru a všech provedených kontrol zabezpečení.
5. Chcete-li zobrazit definici odesílacího kanálu klastru, která je aktuálně používána, 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. Možná budete muset definovat uživatelskou proceduru automatické definice kanálu, CHADEXIT, na správci front odesílatele klastru, pokud jsou správci front na různých platformách.

   Pomocí uživatelské procedury automatické definice kanálu nastavte atribut SecurityExit na vhodný formát pro cílovou platformu.
8. Proveďte implementaci a konfiguraci zabezpečení.

   z/OS **z/OS**

   Modul načtení uživatelské procedury zabezpečení musí být v datové sadě určené v příkazu CSQXLIB DD procedury adresního prostoru iniciátoru kanálu.

   ALW **Systémy AIX, Linux, and Windows**

   - Knihovna DLL pro ukončení zabezpečení musí být v cestě zadané v atributu SCYEXIT definice kanálu.
   - Knihovna dynamických odkazů uživatelské procedury pro automatické definování kanálu musí být uvedena v cestě určené v atributu CHADEXIT definice správce front.

Vynucení opuštění klastru nechtěným správcům front

Vynutí, aby nežádoucí správce front opustil klastr vyvoláním příkazu RESET CLUSTER ve správci front úplného úložiště.

Informace o této úloze

Můžete vynutit, aby nechtěný správce front opustil klastr. Je-li například odstraněn správce front, avšak jeho kanály příjemce klastru jsou stále definovány v klastru. Možná byste se měl uklidit.

Pouze správci front úplného úložiště mají oprávnění k odebrání správce front z klastru.

Poznámka: Přestože použití příkazu RESET CLUSTER vynuceně odebere správce front z klastru, použití příkazu RESET CLUSTER samo o sobě nezabrání opětovnému připojení správce front ke klastru později. Chcete-li se ujistit, že se správce front znovu nepřipojí ke klastru, postupujte podle kroků podrobně uvedených v tématu “Zabránění připojování správců front ke klastru” na stránce 468.

Následujícím postupem vysunete správce front OSLO z klastru NORWAY:

Postup

1. Ve správci front úplného úložiště zadejte příkaz:

   ```
   RESET CLUSTER(NORWAY) QMNAME(OSLO) ACTION(FORCEREMOVE)
   ```
2. Alternativa použijte QMID místo QMNAME v příkazu:

```
RESET CLUSTER(NORWAY) QMID(qmid) ACTION(FORCEREMOVE)
```

Poznámka: QMID je řetězec, takže hodnota qmid by měla být uzavřena jednoduchými uvozovkami, například QMID('FR01_2019-07-15_14.42.42').

Výsledky

Správce front, který je vynucený, se nemění; jeho definice lokálních klastrů se zobrazují, aby byly v klastru. Definice ve všech ostatních správcích front se v tomto klastru nezobrazují.

Zabránění příjmu zpráv správcem front

Můžete zabránit správci front klastru, aby přijímal zprávy, které nemá oprávnění přijímat, pomocí ukončovacích programů.

Informace o této úloze

Zastavení správce front, který je členem klastru, je obtížné definovat z definování fronty. Existuje nebezpečí, že se zbloudilý správce front připojí ke klastru a definuje jeho vlastní instanci jedné z front v klastru. Nyní může přijímat zprávy, které nejsou autorizovány pro příjem. Chcete-li zabránit správci front přijímat zprávy, použijte jednu z následujících voleb uvedených v proceduře.

Procedura

- Ukončovací program kanálu na každém kanálu odesílatele klastru. Ukončovací program používá název připojení k určení vhodnosti cílového správce front, který má být odeslán zprávám.
- Ukončovací program pracovní zátěže klastru, který používá cílové záznamy k určení vhodnosti cílové fronty a správce front k odeslání zpráv.

protokol SSL/TLS

Při konfiguraci zabezpečení TLS pro klastry si uvědomte, že definice kanálu CLUSRCVR je šířena do jiných správců front jako automaticky definovaný kanál CLUSSDR. Pokud kanál CLUSRCVR používá TLS, musíte nakonfigurovat TLS ve všech správcích front, které komunikují pomocí daného kanálu.

Další informace o TLS najdete v tématu “Protokoly zabezpečení TLS v produktu IBM MQ” na stránce 22. Doporučení je obecně použitelné pro kanály klastru, ale možná byste měli věnovat zvláštní pozornost následujícím:

V klastru IBM MQ je určitá definice kanálu CLUSRCVR často šířena do mnoha dalších správců front, kde je transformován na automaticky definované CLUSSDR. Následně se automaticky nadefinovaný CLUSSDR používá ke spuštění kanálu pro CLUSRCVR. Je-li server CLUSRCVR nakonfigurován pro připojení TLS, platí následující pokyny:

- Všichni správci front, kteří chtějí komunikovat s tímto produktem CLUSRCVR , musí mít přístup k podpoře TLS. Toto ustanovení TLS musí podporovat CipherSpec pro kanál.
- Různé správce front, ke kterým byly šířeny automaticky definované odesílací kanály klastru, budou mít k sobě přidruženy odlišné rozlišující názvy. Pokud má být na CLUSRCVR použita kontrola rozlišujícího názvu, musí být nastavena tak, aby všechny rozlišující názvy, které lze přijmout, byly úspěšně porovnány.

  Předpokládejme například, že všichni správci front, kteří budou hostiteli odesílacích kanálů klastru, které se budou připojovat ke konkrétnímu serveru CLUSRCVR, mají přidruženy certifikáty. Předpokládejme také, že rozlišující názvy ve všech těchto certifikátech definují zemi jako UK, organizaci jako IBM, organizační jednotku jako IBM MQ Development a všechny mají společné názvy ve tvaru DEVT.QMnnn, kde nnn je číselný.

V tomto případě hodnota SSLPEER na hodnotě `C=UK, O=IBM, OU=IBM MQ Development, CN=DEVT.QM*` na serveru CLUSRCVR umožní úspěšné připojení všech požadovaných odesílacích kanálů klastru, ale zabrání tomu, aby se nechtěné odesílací kanály klastru připojovaly.

- Pokud jsou použity vlastní řetězce CipherSpec , mějte na paměti, že vlastní formáty řetězců nejsou povoleny na všech platformách. Příklad toho je, že řetězec `CipherSpec RC4_SHA_US` má hodnotu `05` na IBM i , ale není platnou specifikací na systémech AIX, Linux, and Windows . Pokud se tedy v produktu CLUSRCVRpoužívají vlastní parametry SSLCIPH , všechny výsledné automaticky definované kanály odesílatele klastru by měly být umístěny na platformách, na kterých základní podpora TLS implementuje tuto `CipherSpec` a kterou lze zadat s vlastní hodnotou. Pokud nemůžete vybrat hodnotu parametru SSLCIPH , která bude srozumitelná pro celý klastr, budete potřebovat uživatelskou proceduru automatické definice kanálu, abyste ji změnili na něco, čemu budou používány používané platformy. Tam, kde je to možné, použijte textové řetězce `CipherSpec` (například `TLS_RSA_WITH_AES_128_CBC_SHA`).

Parametr SSLCRLNL se vztahuje na jednotlivé správce front a není šířen do jiných správců front v rámci klastru.

Upgrade klastrovaných správců front a kanálů na protokol SSL/TLS

Upgradujte postupně kanály klastru po jedné a změňte všechny kanály CLUSRCVR před kanály CLUSSDR .

Než začnete

Zvažte následující skutečnosti, protože mohou ovlivnit vaši volbu CipherSpec pro klastr:

- Některé CipherSpecs nejsou k dispozici na všech platformách. Buďte opatrní při výběru volby CipherSpec , která je podporována všemi správci front v klastru.
- Některé CipherSpecs mohou být nové ve stávajícím vydání produktu IBM MQ a nejsou podporovány ve starších verzích. Klastr obsahující správce front, kteří jsou spuštěni v různých vydáních produktu MQ , mohou používat pouze specifikace CipherSpecs podporované jednotlivými verzemi.

  Chcete-li použít novou položku CipherSpec v rámci klastru, musíte nejprve migrovat všechny správce front klastru do aktuální verze.
- Některé specifikace CipherSpecs vyžadují použití specifického typu digitálního certifikátu, zejména těch, které používají komponentu Elliptic Curve Cryptography.

Upozornění: Ve správci front, které chcete spojit jako součást klastru, nelze použít směs podepsaných certifikátů Elliptic Curve-podepsaných správců front a certifikátů podepsaných společností RSA.

Správci front v klastru musí používat všechny certifikáty podepsané RSA nebo všechny certifikáty podepsané EC, nikoli směs obou těchto certifikátů.

Další informace viz “Digitální certifikáty a kompatibilita CipherSpec v produktu IBM MQ” na stránce 43.

Proveďte upgrade všech správců front v klastru na produkt IBM MQ V8 nebo vyšší, pokud tyto úrovně ještě nejsou na těchto úrovních. Distribuujte certifikáty a klíče tak, aby TLS fungovalo z každého z nich.

Chcete-li provést upgrade nebo použít některý z aliasů CipherSpecs (ANY_TLS13, ANY_TLS13_OR_HIGHER, ANY_TLS12, ANY_TLS12_OR_HIGHERatd.), musíte provést upgrade všech správců front produktu IBM MQ for Multiplatforms v klastru na produkt IBM MQ 9.1.4 nebo vyšší V 9.2.0 a všechny správce front IBM MQ for z/OS v klastru na server IBM MQ for z/OS 9.2.0 nebo vyšší.

Informace o této úloze

Změňte kanály CLUSRCVR před kanály CLUSSDR .

Postup

1. Přepněte kanály CLUSRCVR na TLS v libovolném pořadí, ve kterém chcete, při změně jedné hodnoty CLUSRCVR a umožněte, aby se změny v klastru procházela dříve, než změníte další.

   Důležité: Ujistěte se, že jste nezměnili opačnou cestu, dokud nejsou změny pro aktuální kanál distribuovány po celém 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: Pro velké klastry může být použití příkazu **REFRESH CLUSTER** pro klastr rušivé, zatímco probíhá, a poté znovu ve 27. denních intervalech, když objekty klastru automaticky odesílají aktualizace stavu všem zúčastněným správcům front. Viz téma Aktualizace velkých klastrů mohou ovlivnit jejich výkon a dostupnost.
3. Použijte příkaz DISPLAY CLUSQMGR , abyste se ujistili, že nová konfigurace zabezpečení byla šířena v celém klastru.
4. Restartujte kanály pro použití TLS a spusťte příkaz REFRESH SECURITY (SSL).

Související pojmy

“Povolení CipherSpecs” na stránce 408
Povolte CipherSpec pomocí parametru **SSLCIPH** v příkazu **DEFINE CHANNEL** nebo **ALTER CHANNEL** MQSC.

“Digitální certifikáty a kompatibilita CipherSpec v produktu IBM MQ” na stránce 43
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

Vypnutí SSL/TLS v klastrovaných správcích a kanálech

Chcete-li protokol TLS vypnout, nastavte parametr SSLCIPH na hodnotu ' '. Zakažte TLS na klastrovaných kanálech jednotlivě, změňte všechny přijímací kanály klastru dříve, než odesílací kanály klastru.

Informace o této úloze

Změňte jeden přijímací kanál klastru současně a umožněte, aby se změny procházela klastrem, a teprve pak změňte další.

Důležité: Ujistěte se, že jste nezměnili opačnou cestu, dokud nejsou změny pro aktuální kanál distribuovány po celém klastru.

Postup

1. Nastavte hodnotu parametru SSLCIPH na ' ', prázdný řetězec v jednoduchém uvozovkách

   IBM i nebo *NONE na IBM i .

   Můžete vypnout TLS na přijímacích kanálech klastru v libovolném pořadí, které chcete.

   Všimněte si, že změny proudí v opačném směru přes kanály, na kterých jste aktivují TLS.
2. Zkontrolujte, zda se nová hodnota odrazí ve všech ostatních správcích front, pomocí příkazu **DISPLAY CLUSQMGR(*)** ALL.
3. Vypněte TLS na všech ručních kanálech odesílatele klastru.

   To nemá žádný vliv na činnost klastru, pokud nepoužijete příkaz **REFRESH CLUSTER** s volbou REPOS(YES).

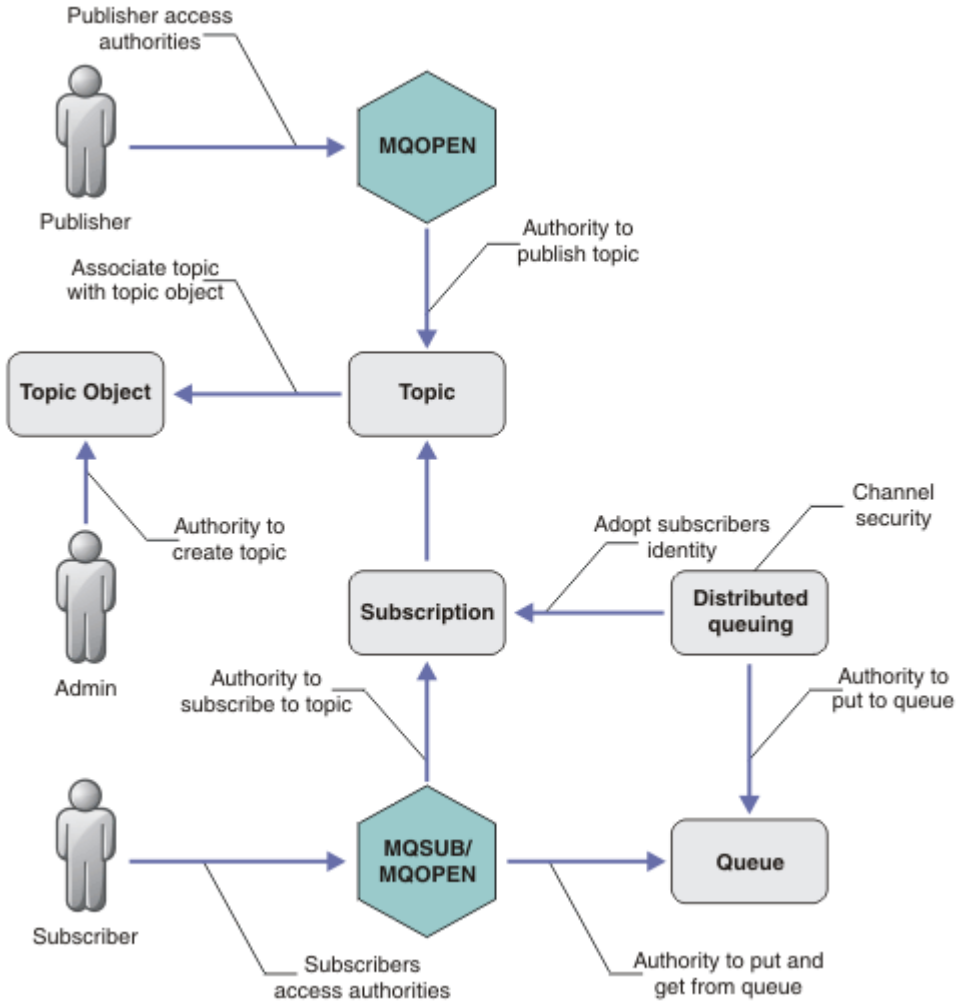
Pro velké klastry může být použití příkazu **REFRESH CLUSTER** pro klastr rušivé, zatímco probíhá jeho zpracování, a poté v pravidelných intervalech, kdy objekty klastru automaticky odesílají aktualizace stavu všem zúčastněným správcům front. Další informace viz Aktualizace ve velkém klastru může ovlivnit výkon a dostupnost klastru .

4. Zastavte a restartujte odesílací kanály klastru.

Zabezpečení publikování/odběru

Komponenty a interakce, které se účastní publikování/odběru, jsou popsány jako úvod do podrobnějších vysvětlení a příkladů, které následují.

Existuje celá řada komponent, které se podílejí na publikování a přihlášení k odběru tématu. Některé ze vztahů zabezpečení mezi nimi jsou ilustrovány v Obrázek 22 na stránce 473 a popsány v následujícím příkladu.



Obrázek 22. Vztahy zabezpečení publikování/odběru mezi různými komponentami

Témata

Témata jsou identifikována pomocí řetězců témat a jsou zpravidla uspořádána do stromů, viz téma Stromy témat. Chcete-li řídit přístup k tématu, je třeba asociovat téma s objektem tématu. Část "Model zabezpečení témat" na stránce 475 vysvětluje, jak zabezpečit témata pomocí objektů témat.

Objekty administrativního tématu

Můžete určovat, kdo má přístup k tématu, a za jakým účelem můžete použít příkaz **setmqaut** se seznamem objektů administrativních témat. Viz příklady, “Udělit uživateli přístup k odběru tématu” na stránce 480 a “Udělit přístup uživateli k publikování v rámci tématu” na stránce 487. z/OS Chcete-li řídit přístup k objektům tématu v systému z/OS, prostudujte si téma Profily pro zabezpečení témat.

Odběry

Přihlaste se k odběru jednoho nebo více témat tak, že vytvoříte odběr dodávající řetězec tématu, který může obsahovat zástupné znaky, aby se shodovaly s řetězci témat v publikacích. Další podrobnosti viz:

Přihlásit se k odběru pomocí objektu tématu

“Přihlášení k odběru pomocí názvu objektu tématu” na stránce 476

Přihlásit se k odběru pomocí tématu

“Přihlášení k odběru pomocí řetězce tématu, ve kterém uzel tématu neexistuje” na stránce 477

Přihlásit se k odběru tématu se zástupnými znaky

“Přihlášení k odběru pomocí řetězce tématu, který obsahuje zástupné znaky” na stránce 478

Odběr obsahuje informace o identitě odběratele a o identitě cílové fronty, na které mají být publikace umístěny. Obsahuje také informace o tom, jak má být publikace umístěna do cílové fronty.

Kromě definování, které odběratelé mají oprávnění přihlásit se k odběru určitých témat, můžete omezit odběry, které mají být používány jednotlivými odběrateli. Můžete také řídit, jaké informace o odběrateli používá správce front, když jsou publikace umístěny do cílové fronty. Viz “Zabezpečení odběru” na stránce 492.

Fronty

Cílová fronta je důležitou frontou, která má být zabezpečena. Je lokální pro odběratele a na ni jsou umístěny publikace, které se shodují s odběrem. Je třeba zvážit přístup k cílové frontě ze dvou perspektiv:

1. Vložení publikování do cílové fronty.
2. Probíhá načítání publikování z cílové fronty.

Správce front vloží do cílové fronty publikování s použitím identity poskytnuté odběratelem. Odběratel nebo program, který byl delegován úlohou publikování publikování, přijímá zprávy z fronty. Viz “Oprávnění k cílovým frontám” na stránce 478.

K dispozici nejsou žádné aliasy objektu tématu, ale jako alias pro objekt tématu můžete použít alias frontu. Pokud tak učiníte a kontrolujete oprávnění k používání tématu pro publikování nebo odběr, zkontroluje správce front oprávnění k použití této fronty.

“Zabezpečení publikování/odběru mezi správci front” na stránce 494

Oprávnění k publikování nebo odběru tématu se kontroluje na lokálním správci front pomocí lokálních identit a autorizací. Autorizace nezávisí na tom, zda je téma definováno, nebo ne, ani místo, 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. Pro fronty můžete dosáhnout stejného výsledku tak, že definujete alias fronty lokálně pro každou klastrovanou frontu.

Správci front došlo k výměně odběrů v klastru. Ve většině konfigurací klastru produktu IBM MQ jsou kanály konfigurovány s produktem PUTAUT=DEF , aby umísťují zprávy do cílových front pomocí oprávnění procesu kanálu. Můžete upravit konfiguraci kanálu tak, aby používala produkt PUTAUT=CTX k vyžadování, aby odebírající uživatel měl oprávnění šířit odběr do jiného správce front v klastru.

Část “Zabezpečení publikování/odběru mezi správci front” na stránce 494 popisuje, jak změnit definice kanálů, aby bylo možné řídit, kdo je oprávněn šířit odběry na jiné servery v klastru.

Autorizace

Můžete použít autorizaci pro objekty témat, stejně jako fronty a další objekty. K dispozici jsou tři autorizace, pub, suba `resume` , které lze použít pouze pro témata. Podrobnosti jsou popsány v části Určení oprávnění pro různé typy objektů.

Volání funkcí

V programech pro publikování a odběr, jako jsou programy ve frontě, jsou při otevírání, vytváření, změnách nebo odstraňování objektů provedeny kontroly autorizace. Při volání produktu MQPUT nebo MQGET MQI nejsou provedeny žádné kontroly, aby bylo možné vkládat a získávat publikování.

Chcete-li publikovat téma, proveďte MQOPEN na téma, které provádí kontroly autorizace. Publikujte zprávy do popisovače tématu pomocí příkazu MQPUT , který neprovádí žádné kontroly autorizace.

Chcete-li se přihlásit k odběru tématu, zpravidla pomocí příkazu MQSUB vytvoříte nebo obnovíte odběr a také chcete-li otevřít cílovou frontu pro příjem publikací. Případně proveďte pro otevření cílové fronty samostatný produkt MQOPEN a poté klepnutím na tlačítko MQSUB vytvořte nebo obnovte odběr.

Bez ohledu na to, jakou výzvu použijete, správce front zkontroluje, zda se můžete přihlásit k odběru tématu a získat výsledné publikace z cílové fronty. Je-li cílová fronta nespravovaná, kontroly autorizace jsou také provedeny tak, aby správce front mohl umisťovat publikace do cílové fronty. Používá identitu, kterou přijal z odpovídajícího odběru. Předpokládá se, že správce front je vždy schopen umisťovat publikování do spravovaných cílových front.

Role

Uživatelé jsou zapojeni do čtyř rolí ve spuštěných aplikacích publikování/odběru:

1. Vydavatel
2. Odběratel
3. Administrátor témat
4. IBM MQ Administrátor-člen skupiny mqm

Definujte skupiny s odpovídajícími autorizacemi, které odpovídají rolím pro publikování, odběr a administraci témat. Poté můžete přiřadit činitele k těmto skupinám, které je opravňují k provedení specifických úloh publikování a odběru.

Kromě toho je třeba rozšířit oprávnění administrativních operací na administrátora front a kanálů zodpovědných za přesun publikací a odběrů.

Model zabezpečení témat

Přidružené atributy zabezpečení mohou mít pouze definované objekty témat. Popis objektů témat naleznete v tématu Objekty administrativního tématu. Atributy zabezpečení určují, zda má být zadané ID uživatele nebo skupina zabezpečení povoleno provádět odběr nebo operaci publikování pro každý objekt tématu.

Atributy zabezpečení jsou přidruženy k příslušnému uzlu administrace ve stromu témat. Je-li během operace odběru nebo publikování provedena kontrola oprávnění pro určité ID uživatele, je udělené oprávnění založeno na atributech zabezpečení přidruženého uzlu stromu témat.

Atributy zabezpečení jsou seznam přístupových práv, který označuje, které oprávnění má určité ID uživatele operačního systému nebo skupiny zabezpečení k objektu tématu.

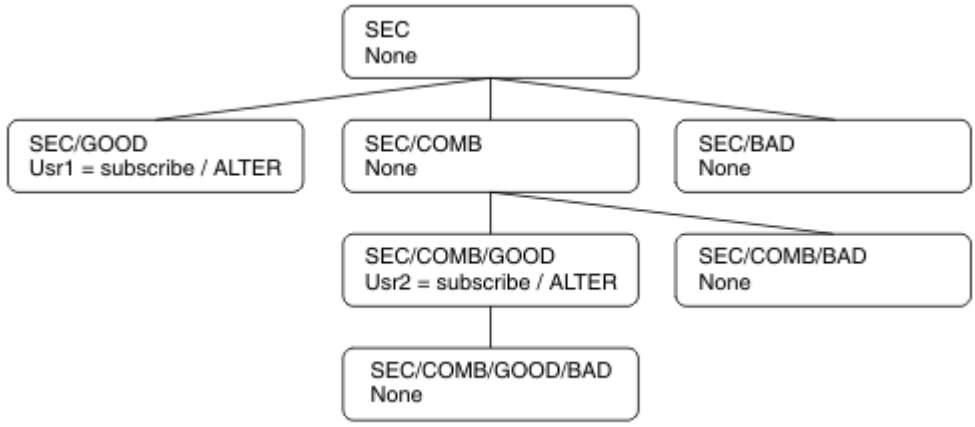
Prohlédněte si následující příklad, kde byly objekty tématu definovány s atributy zabezpečení, nebo s zobrazenými oprávněními:

Tabulka 84. Příklad oprávnění k objektu tématu

Název tématu	Řetězec tématu	Oprávnění-ne z/OS	z/OS oprávnění
SECROOT	SEC	Není	Není

Tabulka 84. Příklad oprávnění k objektu tématu (pokračování)			
Název tématu	**Řetězec tématu**	**Oprávnění-ne z/OS**	**z/OS oprávnění**
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 může být reprezentován následujícím způsobem:



Uvedené příklady uvádějí následující autorizace:

- V kořenovém uzlu stromu /SECžádný uživatel nemá oprávnění na daném uzlu.
- usr1 má uděleno oprávnění k odběru pro objekt /SEC/GOOD
- usr2 má uděleno oprávnění k odběru pro objekt /SEC/COMB/GOOD

Přihlášení k odběru pomocí názvu objektu tématu

Při přihlašování k odběru objektu tématu zadáním názvu MQCHAR48 je umístěn odpovídající uzel ve stromu témat. Pokud atributy zabezpečení přidružené k uzlu indikují, že má uživatel oprávnění přihlásit se k odběru, je přístup udělen.

Pokud uživatel nemá udělen přístup, nadřízený uzel ve stromu určuje, zda má uživatel oprávnění přihlásit se k odběru na úrovni nadřízeného uzlu. Pokud ano, pak je přístup udělen. Není-li tomu tak, bude uvažovaný nadřízený uzel považován za nadřízený. Rekurze pokračuje, dokud se uzel nenastane, který

uděluje oprávnění k odběru pro uživatele. Rekurze se zastaví, když je kořenový uzel považován bez oprávnění, aniž by byl udělen. V druhém případě je přístup odepřen.

Stručně řečeno, pokud libovolný uzel v cestě uděluje oprávnění k odběru u tohoto uživatele nebo aplikace, je odběratel povolen přihlásit se k odběru u daného 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 ID uživatele má oprávnění nebo že skupina zabezpečení operačního systému, jejíž ID uživatele je členem, má oprávnění.

Takže například:

- Pokud se produkt `usr1` pokusí přihlásit odběr s použitím řetězce tématu produktu SEC/GOOD, bude tento odběr povolen, protože ID uživatele bude mít přístup k uzlu přidruženému k tomuto tématu. Pokud se však produkt `usr1` pokusil přihlásit se k odběru pomocí řetězce tématu SEC/COMB/GOOD , odběr by nebyl povolen, protože ID uživatele nemá přístup k uzlu, který je k němu přidružen.
- Pokud se produkt `usr2` pokusí přihlásit k odběru, použije se k odběru řetězce tématu SEC/COMB/GOOD , že má přístup k uzlu přidruženému k tomuto tématu. Pokud se však `usr2` pokus přihlásit k odběru SEC/GOOD , odběr by nebyl povolen, protože ID uživatele nemá přístup k uzlu, který je k němu přidružen.
- Pokud se produkt `usr2` pokusí přihlásit k odběru pomocí řetězce tématu produktu SEC/COMB/GOOD/BAD , může být odběr povolen, protože má ID uživatele přístup k nadřízenému uzlu SEC/COMB/GOOD.
- Pokud se produkt `usr1` nebo `usr2` pokusí přihlásit k odběru pomocí řetězce tématu produktu /SEC/COMB/BAD, nebude povolen, protože nemají přístup k uzlu tématu, který je k němu přidružen, nebo k nadřazeným uzlům daného tématu.

Operace odběru uvádějící název objektu tématu, který neexistuje, má za následek chybu MQRC_UNKNOWN_OBJECT_NAME.

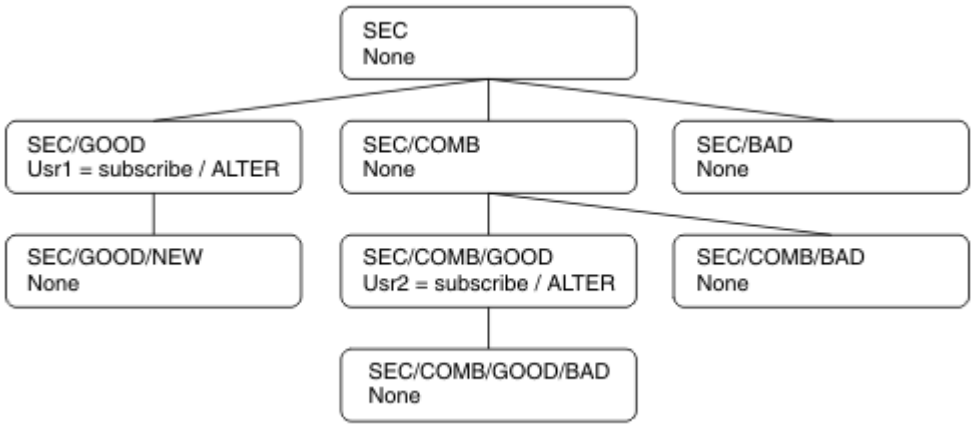
Přihlášení k odběru pomocí řetězce tématu, ve kterém uzel tématu existuje

Chování je stejné jako při zadávání tématu pomocí názvu objektu MQCHAR48 .

Přihlášení k odběru pomocí řetězce tématu, ve kterém uzel tématu neexistuje

Uvažte případ odběru aplikace a určete řetězec tématu představující uzel tématu, který aktuálně neexistuje ve stromu témat. Kontrola oprávnění se provádí tak, jak je uvedeno v předchozí sekci. Kontrola se spustí s nadřazeným uzlem, který je reprezentován řetězcem tématu. Je-li oprávnění uděleno, bude ve stromu témat vytvořen nový uzel reprezentující řetězec tématu.

Produkt `usr1` se například 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 objekt tématu, ke kterému nejsou přímo přidruženy žádné atributy zabezpečení. Atributy jsou zděděny od svého nadřízeného objektu.



Přihlášení k odběru pomocí řetězce tématu, který obsahuje zástupné znaky

Zvažte možnost přihlášení k odběru s použitím řetězce tématu, který obsahuje zástupný znak. Kontrola oprávnění se provádí vůči uzlu ve stromu témat, který odpovídá úplné části řetězce tématu.

Pokud se tedy aplikace přihlašuje k odběru produktu SEC/COMB/GOOD/*, provede se kontrola oprávnění tak, jak je uvedeno v předchozích dvou sekcích uzlu SEC/COMB/GOOD ve stromu témat.

Podobně platí, že pokud se aplikace potřebuje přihlásit k odběru SEC/COMB/*/GOOD, provede se kontrola oprávnění na uzlu SEC/COMB.

Oprávnění k cílovým frontám

Při přihlašování k odběru tématu je jedním z parametrů popisovač hobj fronty, který byl otevřen pro výstup pro příjem publikací.

Není-li parametr hobj zadán, ale je prázdný, je vytvořena spravovaná fronta, pokud jsou splněny následující podmínky:

- Byla zadána volba MQSO_MANAGED .
- Odběr neexistuje.
- Je zadán parametr Create.

Pokud je hobj prázdný a měníte nebo obnovujete existující odběr, cílová fronta může být buď spravovaná, nebo nespravovaná.

Aplikace nebo uživatel, který vytváří požadavek produktu MQSUB , musí mít oprávnění pro vkládání zpráv do cílové fronty, jakou má k dispozici; v důsledku toho oprávnění k publikování zpráv vložených do této fronty. Kontrola oprávnění se řídí podle existujících pravidel pro kontrolu zabezpečení fronty.

Kontrola zabezpečení zahrnuje alternativní ID uživatele a kontroly zabezpečení kontextu tam, kde je to požadováno. Chcete-li být schopni nastavit libovolné pole kontextu identity, musíte zadat volbu MQSO_SET_IDENTITY_CONTEXT stejně jako volbu MQSO_CREATE nebo MQSO_ALTER . Na požadavek MQSO_RESUME nemůžete nastavit žádné z kontextových polí Identita.

Je-li cílem spravovaná fronta, žádné kontroly zabezpečení se neprovedou u spravovaného cíle. Pokud máte možnost přihlásit se k odběru tématu, předpokládá se, že můžete používat spravovaná místa určení.

Publikování s použitím názvu tématu nebo řetězce tématu, ve kterém uzel tématu existuje

Model zabezpečení pro publikování je stejný jako u odběru u odběru, s výjimkou zástupných znaků. Publikace neobsahují zástupné znaky; takže zde není žádný případ řetězce tématu, který obsahuje zástupné znaky, které byste mohli vzít v úvahu.

Oprávnění k publikování a odběru jsou odlišné. Uživatel nebo skupina může mít oprávnění k provedení jednoho, aniž by musel být schopen provést jinou operaci.

Při publikování do objektu tématu zadáním názvu MQCHAR48 nebo řetězce tématu bude umístěn odpovídající uzel ve stromu témat. Pokud atributy zabezpečení přidružené k uzlu tématu indikují, že má uživatel oprávnění k publikování, pak je přístup udělen.

Není-li přístup udělen, určuje nadřízený uzel ve stromu, zda má uživatel oprávnění k publikování na této úrovni. Pokud ano, pak je přístup udělen. Pokud tomu tak není, rekurze pokračuje, dokud se nenastane uzel, který uděluje uživateli oprávnění k publikování. Rekurze se zastaví, když je kořenový uzel považován bez oprávnění, aniž by byl udělen. V druhém případě je přístup odepřen.

Stručně řečeno, pokud libovolný uzel v cestě uděluje oprávnění publikovat tomuto uživateli nebo aplikaci, vydavatel může publikovat v daném uzlu nebo kdekoliv pod tímto uzlem ve stromu témat.

Publikování s použitím názvu tématu nebo řetězce tématu, ve kterém uzel tématu neexistuje

Stejně jako v případě operace odběru, při publikování aplikace se zadáním řetězce tématu představujícího uzel tématu, který aktuálně neexistuje ve stromu témat, provede se kontrola oprávnění počínaje nadřazeným uzlem uzlu představovaného řetězcem tématu. Je-li oprávnění uděleno, bude ve stromu témat vytvořen nový uzel reprezentující řetězec tématu.

Publikování s použitím aliasu fronty, který je interpretováno jako objekt tématu

Pokud publikujete pomocí alias fronty, který je interpretováno jako objekt tématu, dojde ke kontrole zabezpečení jak ve frontě aliasů, tak v základním tématu, na které se tento objekt řeší.

Kontrola zabezpečení ve frontě aliasů ověřuje, zda má uživatel oprávnění k umístění zpráv do této fronty aliasů, a kontrola zabezpečení na daném tématu ověřuje, zda je uživatel může do tohoto tématu publikovat. Je-li alias fronta přeložena do jiné fronty, nejsou prováděny žádné kontroly v příslušné frontě. Kontrola oprávnění se provádí odlišně pro témata a fronty.

Zavření odběru

Pokud jste nevytvořili odběr pod tímto popisovačem, je třeba provést další kontrolu zabezpečení, pokud jste nevytvořili odběr pomocí volby MQCO_REMOVE_SUB .

Kontrola zabezpečení se provádí, aby se zajistilo, že máte správné oprávnění k provedení této akce, jako je akce při odebrání odběru. Pokud atributy zabezpečení přidružené k uzlu tématu indikují, že má uživatel oprávnění, pak je přístup udělen. Pokud tomu tak není, je nadřízený uzel ve stromu považován za účelem určení, zda má uživatel oprávnění k uzavření odběru. Rekurze pokračuje, dokud není uděleno žádné oprávnění nebo je dosažen kořenový uzel.

Definování, změna a odstranění odběru

Při vytvoření administrativně odběru se neprovádějí žádné kontroly zabezpečení odběru, místo použití požadavku rozhraní API produktu MQSUB . Administrátorovi bylo toto oprávnění uděleno prostřednictvím příkazu.

Jsou provedeny kontroly zabezpečení, aby bylo zajištěno, že publikování lze vložit do cílové fronty přidružené k odběru. Kontroly jsou prováděny stejným způsobem jako u požadavku MQSUB .

ID uživatele, které se používá pro tyto kontroly zabezpečení, závisí na vydávaný příkaz. Je-li zadán argument **SUBUSER** , ovlivní to způsob kontroly, jak ukazuje Tabulka 85 na stránce 479:

Tabulka 85. ID uživatele používaná pro kontroly zabezpečení pro příkazy

Příkaz	SUBUSER zadán a prázdný	SUBUSER zadán a dokončen	SUBUSER není zadán
	Použít ID administrátora		Použít ID uživatele z odběru LIKE
	Použít ID administrátora		Použijte ID.DEFAULT.SU uživateleB -je-li z SYSTEMprázdné, použijte ID administrátora.

Tabulka 85. ID uživatele používaná pro kontroly zabezpečení pro příkazy (pokračování)			
Příkaz	**SUBUSER zadán a prázdný**	**SUBUSER zadán a dokončen**	**SUBUSER není zadán**
	Použít ID administrátora		Použít ID uživatele z existujícího odběru

Jediná kontrola zabezpečení provedená při odstranění odběrů pomocí příkazu DELETE SUB je kontrola zabezpečení příkazu.

Příklad nastavení zabezpečení pro publikování/odběr

Tato sekce popisuje scénář, který má přístup k řízení přístupu k tématům takovým způsobem, který umožňuje použití ovladače zabezpečení podle potřeby.

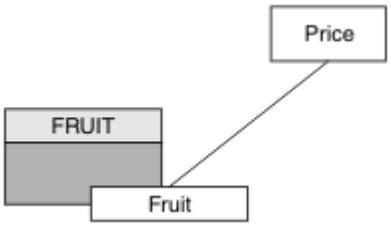
Udělit uživateli přístup k odběru tématu

Toto téma je první v seznamu úloh, které vám říká, jak udělit přístup k tématům více než jedním uživatelem.

Informace o této úloze

Tato úloha předpokládá, že neexistují žádné administrativní objekty témat, ani žádné profily nebyly definovány pro odběr nebo publikování. Aplikace vytvářejí nové odběry, spíše než aby obnovila existující, a provádí se tak pouze pomocí řetězce tématu.

Aplikace může provést odběr zadáním objektu tématu nebo řetězce tématu nebo kombinací obou těchto typů. Bez ohledu na způsob, jakým aplikace vybere aplikace, má tento účinek ve stromu témat učinit odběr v určitém bodě. Je-li tento bod ve stromu témat reprezentován objektem administrativního tématu, je profil zabezpečení zkontrolován na základě názvu daného objektu tématu.



Obrázek 23. Příklad přístupu k objektu tématu

Tabulka 86. Příklad přístupu k objektu tématu		
Téma	**Je vyžadován přístup pro**	**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 produktu USER1 k odběru tématu `"Price/Fruit"` tím, že udělíte uživateli přístup k profilu produktu `hlq.SUBSCRIBE.FRUIT` . Toto proveďte pomocí následujících příkazů obslužného programu RACF :

  ```
  RDEFINE MXTOPIC hlq.SUBSCRIBE.FRUIT UACC(NONE)
  PERMIT hlq.SUBSCRIBE.FRUIT CLASS(MXTOPIC) ID(USER1) ACCESS(ALTER)
  ```

- Ostatní platformy:

  Udělte přístup k produktu USER1 k odběru tématu `"Price/Fruit"` tím, že udělíte uživateli přístup 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 produkt USER1 pokusí přihlásit k odběru tématu `"Price/Fruit"` , výsledek je úspěšný.

Když se produkt USER2 pokusí přihlásit k odběru tématu `"Price/Fruit"` , výsledkem je selhání zprávy `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 ostatních platformách následující autorizační událost:

  ```
  MQRC_NOT_AUTHORIZED
  ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
  UserIdentifier        USER2
  AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
  TopicString           "Price/Fruit"
  ```

- IBM i V systému IBMi následující autorizační událost:

  ```
  MQRC_NOT_AUTHORIZED
  ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
  UserIdentifier        USER2
  AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
  TopicString           "Price/Fruit"
  ```

Všimněte si, že toto je obrázek toho, co vidíte; ne všechna pole.

Udělte uživateli přístup k odběru tématu hlouběji do stromu.

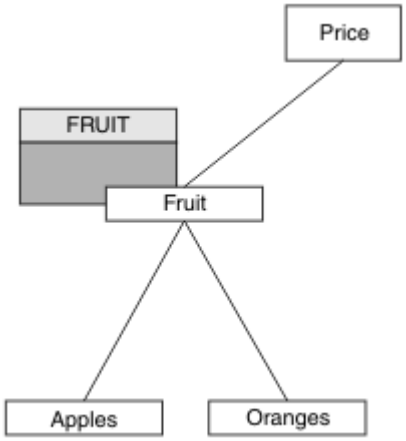
Toto téma je druhé v seznamu úloh, které vás informují o tom, jak udělit přístup k tématům více uživateli.

Než začnete

Toto téma používá nastavení popsané v části “Udělit uživateli přístup k odběru tématu” na stránce 480.

Informace o této úloze

Pokud bod ve stromu témat, v němž aplikace provádí odběr, není reprezentován administrativním objektem tématu, přesuňte strom tak, aby byl umístěn nejbližší nadřízený objekt administrativního tématu. Profil zabezpečení je zkontrolován na základě názvu daného objektu tématu.



Obrázek 24. Příklad udělení přístupu k tématu ve stromu témat

Tabulka 87. Požadavky na přístup pro ukázková témata a objekty témat

Téma	Je vyžadován přístup pro	Objekt tématu
Cena	Žádný uživatel	Není
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 produktu `hlq.SUBSCRIBE.FRUIT` na serveru z/OS a k odběru přístupu k odběru profilu produktu FRUIT na jiných platformách. Tento jeden profil také uděluje přístup USER1 k odběru `"Price/Fruit/Apples"`, `"Price/Fruit/Oranges"` a `"Price/Fruit/#"`.

Když se produkt USER1 pokusí přihlásit k odběru tématu `"Price/Fruit/Apples"` , výsledek je úspěšný.

Když se produkt USER2 pokusí přihlásit k odběru tématu `"Price/Fruit/Apples"` , výsledkem je selhání zprávy `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 ostatních platformách následující autorizační událost:

```
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 na z/OS , jsou totožné s těmi, které jste obdrželi v předchozí úloze, protože stejné objekty tématu a profily ovládají přístup.
- Zpráva události, kterou obdržíte na jiných platformách, je podobná té, která byla přijata v předchozí úloze, ale skutečný řetězec tématu se liší.

Udělte jinému uživateli přístup k odběru pouze tématu hlouběji do stromu.

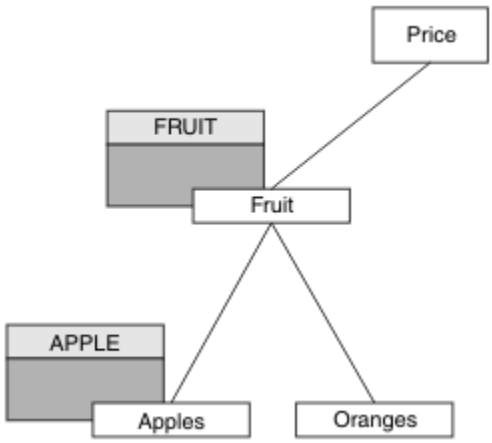
Toto téma je třetí ze seznamu úloh, které vám říkají, jak udělit přístup k odběru témat více než jedním uživatelem.

Než začnete

Toto téma používá nastavení popsané v části “Udělte uživateli přístup k odběru tématu hlouběji do stromu.” na stránce 481.

Informace o této úloze

V předchozí úloze byl USER2 odmítnut přístup k tématu `"Price/Fruit/Apples"`. Toto téma informuje o tom, jak udělit přístup k tomuto tématu, ale ne k jiným tématům.



Obrázek 25. Udělení přístupu ke specifickým tématům v rámci stromu témat

Tabulka 88. Požadavky na přístup pro ukázková témata a objekty témat

Téma	Je vyžadován přístup pro	Objekt tématu
Cena	Žádný uživatel	Není
Cena/Ovoce	USER1	OVOCE
Cena/Ovoce/Jablka	USER1 a USER2	Apple
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 přístupu uživatele k profilu produktu `hlq.SUBSCRIBE.FRUIT` .

     Tento jediný profil také udělil USER1 přístup k odběru `"Price/Fruit/Oranges"` `"Price/Fruit/#"` a tento přístup zůstává i s přidáním nového objektu tématu a s přidruženými profily.

     Udělte přístup k produktu USER2 k odběru tématu `"Price/Fruit/Apples"` tím, že udělíte uživateli přístup k profilu produktu `hlq.SUBSCRIBE.APPLE` . Toto proveďte pomocí následujících příkazů obslužného programu 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"` tím, že uživateli udělil přístup k odběru profilu `FRUIT` .

     Tento jediný profil také udělil USER1 přístup k odběru `"Price/Fruit/Oranges"` a `"Price/Fruit/#"`a tento přístup zůstává dokonce i s přidáním nového objektu tématu a s tím, že k němu jsou přidruženy profily.

     Udělte přístup k produktu USER2 k přihlášení k odběru tématu `"Price/Fruit/Apples"` tím, že uživateli přidělíte přístup k odběru pro profil produktu `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

Pokud se v produktu z/OSpři pokusu USER1 o přihlášení k odběru tématu `"Price/Fruit/Apples"` nezdaří první kontrola zabezpečení v profilu produktu `hlq.SUBSCRIBE.APPLE` , ale při přesunu stromu profilu produktu `hlq.SUBSCRIBE.FRUIT` umožňuje přihlášení k odběru USER1 , odběr je úspěšný a pro volání MQSUB se neodešle žádný návratový kód. Zpráva RACF `ICH` se však vygeneruje pro první kontrolu:

```
ICH408I USER(USER1   ) ...
  hlq.SUBSCRIBE.APPLE ...
```

Když se produkt USER2 pokusí přihlásit k odběru tématu `"Price/Fruit/Apples"` , výsledek je úspěšný, protože kontrola zabezpečení proběhne na prvním profilu.

Když se produkt USER2 pokusí přihlásit k odběru tématu `"Price/Fruit/Oranges"` , výsledkem je selhání zprávy `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 následující autorizační událost:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit/Oranges"
```

- IBM i V systému IBMi následující autorizační událost:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit/Oranges"
```

Nevýhodou tohoto nastavení je to, že v systému z/OSobdržíte na konzole další zprávy produktu `ICH` . Tomuto se můžete vyhnout, pokud jste strom témat zabezpečili jiným způsobem.

Změnit řízení přístupu tak, aby se předešlo dalším zprávám

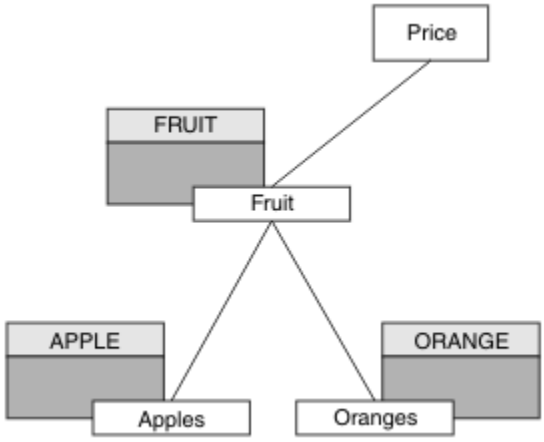
Toto téma je čtvrté v seznamu úloh, které vám sdělují, jak udělit přístup k odběru témat více uživateli a vyhnout se dalším zprávám RACF ICH408I na serveru z/OS.

Než začnete

Toto téma vylepšuje nastavení popsané v tématu “Udělte jinému uživateli přístup k odběru pouze tématu hlouběji do stromu.” na stránce 483 , takže se vyhnete dalším chybovým zprávám.

Informace o této úloze

Toto téma vám říká, jak udělit přístup k tématům hlouběji ve stromu a jak odstranit přístup k tématu níže ve stromu, když jej žádný uživatel nepotřebuje.



Obrázek 26. Příklad udělení řízení přístupu pro zamezení dalších zpráv.

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 tomuto profilu přístup a existující profily. Toto proveďte pomocí následujících příkazů obslužného programu 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 **IBM i**

     ```
     GRTMQAUT OBJ(ORANGE) OBJTYPE(*TOPIC) USER(USER1) AUT(*SUB)
     GRTMQAUT OBJ(APPLE) OBJTYPE(*TOPIC) USER(USER1) AUT(*SUB)
     ```

Výsledky

Pokud se v produktu z/OSpokusí produkt USER1 přihlásit k odběru tématu `"Price/Fruit/Apples"` , je první kontrola zabezpečení profilu `hlq.SUBSCRIBE.APPLE` úspěšná.

Podobně platí, že když se produkt USER2 pokusí přihlásit k odběru tématu `"Price/Fruit/Apples"` , výsledek je úspěšný, protože kontrola zabezpečení proběhne na prvním profilu.

Když se produkt USER2 pokusí přihlásit k odběru tématu `"Price/Fruit/Oranges"` , výsledkem je selhání zprávy `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 ostatních platformách následující autorizační událost:

  ```
  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 následující autorizační událost:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      ORANGE, FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit/Oranges"
```

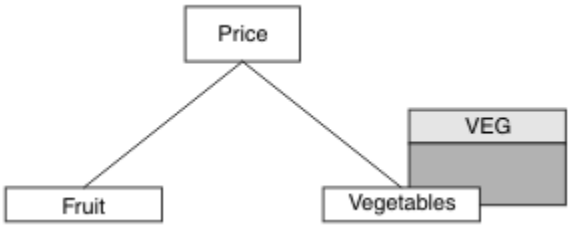
Udělit přístup uživateli k publikování v rámci tématu

Toto téma je první v seznamu úloh, které vám říká, jak udělit přístup k publikačním tématům více než jednoho uživatele.

Informace o této úloze

Tato úloha předpokládá, že na pravé straně stromu témat neexistují žádné objekty administrativních témat, ani nejsou definovány žádné profily pro publikování. Předpokládá se, že vydavatelé používají pouze řetězec tématu.

Aplikace může publikovat do tématu poskytnutím objektu tématu nebo řetězce tématu nebo kombinací obou těchto témat. Bez ohledu na způsob, jakým aplikace vybere aplikace, bude tento efekt ve stromu témat publikován v určitém bodě. Je-li tento bod ve stromu témat reprezentován objektem administrativního tématu, je profil zabezpečení zkontrolován na základě názvu daného objektu tématu. Příklad:



Obrázek 27. Udělení přístupu pro publikování k tématu

Tabulka 89. Příklad požadavků na přístup pro publikování

Téma	Požadovaný 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 produktu USER1 k publikování v rámci tématu `"Price/Vegetables"` udělením přístupu uživatele k profilu produktu `hlq.PUBLISH.VEG` . Toto proveďte pomocí následujících příkazů obslužného programu RACF :

     ```
     RDEFINE MXTOPIC hlq.PUBLISH.VEG UACC(NONE)
     PERMIT hlq.PUBLISH.VEG CLASS(MXTOPIC) ID(USER1) ACCESS(UPDATE)
     ```

- Ostatní platformy:

  Udělte přístup k produktu USER1 k publikování v rámci tématu `"Price/Vegetables"` udělením přístupu uživatele k profilu produktu 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 produkt USER1 pokusí o publikování do tématu `"Price/Vegetables"` , výsledek je úspěšný; to znamená, že volání MQOPEN je úspěšné.

Když se příkaz 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 ostatních platformách následující autorizační událost:

  ```
  MQRC_NOT_AUTHORIZED
  ReasonQualifier      MQRQ_OPEN_NOT_AUTHORIZED
  UserIdentifier        USER2
  AdminTopicNames      VEG, SYSTEM.BASE.TOPIC
  TopicString           "Price/Vegetables"
  ```

- IBM i V systému IBMi následující autorizační událost:

  ```
  MQRC_NOT_AUTHORIZED
  ReasonQualifier      MQRQ_OPEN_NOT_AUTHORIZED
  UserIdentifier        USER2
  AdminTopicNames      VEG, SYSTEM.BASE.TOPIC
  TopicString           "Price/Vegetables"
  ```

Všimněte si, že toto je obrázek toho, co vidíte; ne všechna pole.

Udělte uživateli přístup k tématu hlouběji do stromu.

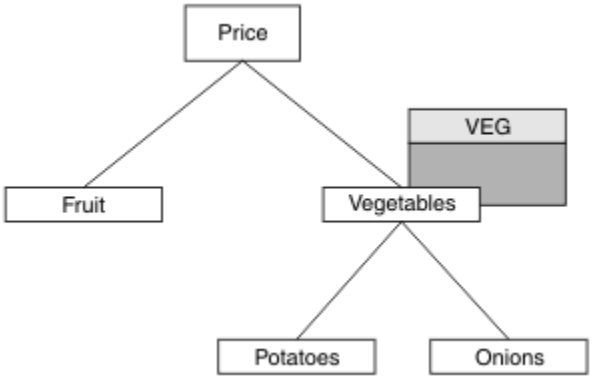
Toto téma je druhé v seznamu úloh, které vás informují o tom, jak udělit přístup k publikačním tématům více uživateli než jednomu uživateli.

Než začnete

Toto téma používá nastavení popsané v části “Udělit přístup uživateli k publikování v rámci tématu” na stránce 487.

Informace o této úloze

Pokud bod ve stromu témat obsahující publikování aplikace není reprezentován administrativním objektem tématu, přesuňte strom tak, aby byl umístěn nejbližší nadřízený objekt administrativního tématu. Profil zabezpečení je zkontrolován na základě názvu daného objektu tématu.



Obrázek 28. Udělení přístupu pro publikování k tématu v rámci stromu témat

Tabulka 90. Příklad požadavků na přístup pro publikování

Téma	Je vyžadován přístup pro	Objekt tématu
Cena	Žádný uživatel	Není
Cena/Zelenina	USER1	VEG.
Cena/Zelenina/Potatony	USER1	
Cena/Zelenina/Onivy	USER1	

V předchozí úloze USER1 byl udělen přístup k publičnímu tématu `"Price/Vegetables/Potatoes"` tím, že mu udělíte přístup k profilu produktu `hlq.PUBLISH.VEG` na serveru z/OS nebo publikoval přístup k profilu produktu VEG na jiných platformách. Tento jeden profil také uděluje přístup USER1 k publikaci v `"Price/Vegetables/Onions"`.

Když se USER1 pokusí publikovat v tématu `"Price/Vegetables/Potatoes"` , výsledek je úspěšný; to je volání MQOPEN je úspěšné.

Když se produkt USER2 pokusí přihlásit k odběru tématu `"Price/Vegetables/Potatoes"` , výsledek se nezdařil; volání MQOPEN se nezdaří 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 ostatních platformách následující autorizační událost:

```
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 na z/OS , jsou totožné s těmi, které jste obdrželi v předchozí úloze, protože stejné objekty tématu a profily ovládají přístup.
- Zpráva události, kterou obdržíte na jiných platformách, je podobná té, která byla přijata v předchozí úloze, ale skutečný řetězec tématu se liší.

Udělit přístup pro publikování a odběr

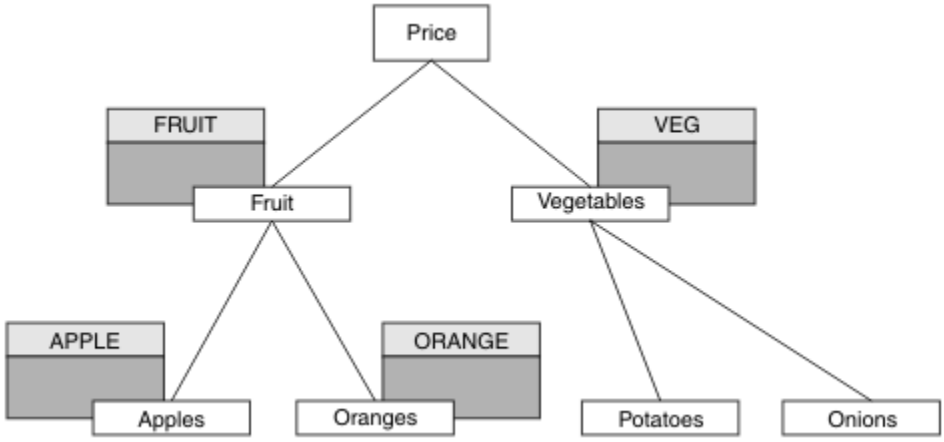
Toto téma je poslední v seznamu úloh, které vás informují o tom, jak udělit přístup k publikování a k odběru témat více než jedním uživatelem.

Než začnete

Toto téma používá nastavení popsané v části “Udělte uživateli přístup k tématu hlouběji do stromu.” na stránce 488.

Informace o této úloze

V předchozí úloze USER1 byl poskytnut přístup k odběru tématu `"Price/Fruit"`. Toto téma vám sděluje, jak udělit přístup tomuto uživateli k publikování v tomto tématu.



Obrázek 29. Udělení přístupu pro publikování a odběr

Tabulka 91. Příklad požadavků na publikování a přihlášení k odběru

Téma	Je vyžadován přístup pro	Požadovaný přístup pro publikování	Objekt tématu
Cena	Žádný uživatel	Žádný uživatel	Není
Cena/Ovoce	USER1	USER1	OVOCE
Cena/Ovoce/Jablka	USER1 a USER2		Apple
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 přístupu uživatele k profilu produktu `hlq.SUBSCRIBE.FRUIT` .

Chcete-li publikovat na téma `"Price/Fruit"` , udělte přístup k USER1 profilu `hlq.PUBLISH.FRUIT` . Toto proveďte pomocí následujících příkazů obslužného programu RACF :

```
RDEFINE MXTOPIC hlq.PUBLISH.FRUIT UACC(NONE)
PERMIT hlq.PUBLISH.FRUIT CLASS(MXTOPIC) ID(USER1) ACCESS(ALTER)
```

- Ostatní platformy:

  Udělte přístup k produktu USER1 k publikování na téma `"Price/Fruit"` tím, že uživateli udělíte přístup pro publikování k profilu produktu FRUIT . Proveďte to pomocí příkazu autorizace pro platformu:

  ALW **Systémy AIX, Linux, and Windows**

  ```
  setmqaut -t topic -n FRUIT -p USER1 +pub
  ```

  IBM i **IBM i**

  ```
  GRTMQAUT OBJ(FRUIT) OBJTYPE(*TOPIC) USER(USER1) AUT(*PUB)
  ```

Výsledky

On z/OS, when USER1 attempts to publish to topic `"Price/Fruit"` the security check on the MQOPEN call passes.

Když se příkaz USER2 pokusí o publikaci na téma `"Price/Fruit"` , výsledkem je selhání se zprávou `MQRC_NOT_AUTHORIZED` společně 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.FRUIT ...

  ICH408I USER(USER2   ) ...
    hlq.PUBLISH.SYSTEM.BASE.TOPIC ...
  ```

- ALW Na platformách AIX, Linux, and Windows následující autorizační událost:

  ```
  MQRC_NOT_AUTHORIZED
  ReasonQualifier      MQRQ_OPEN_NOT_AUTHORIZED
  UserIdentifier        USER2
  AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
  TopicString           "Price/Fruit"
  ```

- IBM i V systému IBM inásledující autorizační událost:

  ```
  MQRC_NOT_AUTHORIZED
  ReasonQualifier      MQRQ_OPEN_NOT_AUTHORIZED
  UserIdentifier        USER2
  AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
  TopicString           "Price/Fruit"
  ```

Po dokončení celé sady těchto úloh poskytne produkt USER1 a USER2 následující přístupová oprávnění pro publikování a přihlášení k odběru témat uvedených v následujících tématech:

Tabulka 92. Úplný seznam přístupových oprávnění vedoucích k příkladům zabezpečení			
Téma	**Je vyžadován přístup pro**	**Požadovaný přístup pro publikování**	**Objekt tématu**
Cena	Žádný uživatel	Žádný uživatel	Není
Cena/Ovoce	USER1	USER1	OVOCE
Cena/Ovoce/Jablka	USER1 a USER2		Apple
Cena/Ovoce/Pomeranče	USER1		ORANŽOVÁ
Cena/Zelenina		USER1	VEG.
Cena/Zelenina/Potatony			
Cena/Zelenina/Onivy			

Pokud máte různé požadavky pro zabezpečení přístupu na různých úrovních ve stromu témat, pečlivé plánování zajišťuje, že v protokolu konzoly produktu z/OS nebude docházet k nadbytečným varováním zabezpečení. Nastavení zabezpečení na správné úrovni v rámci stromu se vyhýbá zavádějícím zprávám zabezpečení.

Zabezpečení odběru

OPRÁVNĚNÍ UŽIVATELE MQSO_ALTERNATE_USER_AUTHORITY

Pole ID AlternateUserobsahuje identifikátor uživatele, který se má použít k ověření tohoto volání MQSUB. Volání může být úspěšné pouze v případě, že je tento identifikátor AlternateUserautorizován k přihlášení k odběru tématu s určenými volbami přístupu bez ohledu na to, zda je identifikátor uživatele, pod kterým je aplikace spuštěna, oprávněn tak učinit.

KONTEXT MQSO_SET_IDENTITY_CONTEXT

Cílem odběru je použít data evidence a údaje o identitě aplikace zadané v polích PubAccountinga PubApplIdentityData .

Je-li tato volba zadána, provede se stejná kontrola autorizace jako v případě, že k cílové frontě bylo přistupováno pomocí volání MQOPEN s MQOO_SET_IDENTITY_CONTEXT, s výjimkou případu, kdy je použita volba MQSO_MANAGED také v tom případě, že v cílové frontě není žádná kontrola autorizace.

Není-li tato volba zadána, budou k publikacím odeslaným pro tohoto odběratele přidruženy výchozí informace o kontextu:

Tabulka 93. Výchozí informace o kontextu publikování	
Pole v MQMD	**Použitá hodnota**
UserIdentifier	ID uživatele přidružené k odběru (viz pole SUBUSER v DISPLAY SBSTATUS) v době, kdy byla publikace vytvořena.

Tabulka 93. Výchozí informace o kontextu publikování (pokračování)	
Pole v MQMD	**Použitá hodnota**
AccountingToken	Je-li to možné, určeno z prostředí; v opačném případě nastavte hodnotu MQACT_NONE.
ApplIdentityData	Nastavit na mezery.

Tato volba je platná pouze s MQSO_CREATE a MQSO_ALTER. Pokud se používá s MQSO_RESUME, pole PubAccountingToken a PubApplIdentityData se ignorují, takže tato volba nemá žádný efekt.

Pokud je odběr změněn bez použití této volby, pokud již odběr poskytl informace o kontextu identity, jsou pro pozměněný odběr generovány výchozí informace o kontextu.

Je-li odběr povolující použití jiných ID uživatelů s volbou MQSO_ANY_USERID obnoven jiným ID uživatele, bude vygenerován výchozí kontext identity pro nové ID uživatele, které nyní vlastní odběr, a budou doručena všechna následující publikování obsahující nový kontext identity.

AlternateSecurityId

Jedná se o identifikátor zabezpečení předávaný spolu s ID AlternateUserk autorizační službě, aby bylo možné provádět odpovídající kontroly autorizace. ID AlternateSecurityID se používá pouze v případě, že je zadán parametr MQSO_ALTERNATE_USER_AUTHORITY a pole ID AlternateUsernení zcela prázdné do prvního znaku null nebo do konce pole.

Volba odběru MQSO_ANY_USERID

Je-li zadáno MQSO_ANY_USERID, identita odběratele není omezena pouze na jedno ID uživatele. To umožňuje jakémukoli uživateli změnit nebo obnovit odběr, když mají odpovídající oprávnění. Pouze jeden uživatel může mít odběr v jednom okamžiku. Pokus o pokračování v použití odběru, který je aktuálně používán jinou aplikací, způsobí selhání volání funkce MQRC_SUBSCRIPTION_IN_USE.

Chcete-li tuto volbu přidat do existujícího odběru, musí volání MQSUB (pomocí funkce 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 se zdaří pouze v případě, že má nové ID uživatele oprávnění k odběru daného tématu. Po úspěšném dokončení se budoucí publikace k tomuto odběrateli umístí do fronty odběratele s použitím nového ID uživatele nastaveného v publikování.

ID UŽIVATELE MQSO_FIXED_USERID

Je-li zadáno MQSO_FIXED_USERID, může být odběr pouze změněn nebo obnoven pouze jedním vlastníkem ID uživatele. Toto ID uživatele je posledním ID uživatele pro změnu odběru, který tuto volbu nastavil, a tím odebrání volby MQSO_ANY_USERID, nebo pokud nedošlo k žádným změnám, je to ID uživatele, které vytvořil odběr.

Pokud se příkazové slovo MQSUB odkazuje na existující odběr se sadou MQSO_ANY_USERID a pozmění odběr (pomocí MQSO_ALTER) pro použití volby MQSO_FIXED_USERID, je nyní ID uživatele odběru opraveno v tomto novém ID uživatele. Volání se zdaří pouze tehdy, má-li nové ID uživatele oprávnění přihlásit se k odběru tématu.

Pokud ID uživatele záznamu MQSO_FIXED_USERID jiný než ten, který je zaznamenaný jako vlastník odběru, způsobí selhání volání funkce MQRC_IDENTITY_MISMATCH. Vlastnící ID uživatele odběru lze zobrazit pomocí příkazu DISPLAY SBSTATUS.

Není-li zadán parametr MQSO_ANY_USERID nebo MQSO_FIXED_USERID, je výchozí hodnota MQSO_FIXED_USERID.

Zabezpečení publikování/odběru mezi správci front

Interní zprávy publikování/odběru, jako jsou například proxy odběry a publikace, jsou vloženy do systémových front publikování/odběru s použitím běžných pravidel zabezpečení kanálu. Informace a diagramy v tomto tématu zdůrazňují různé procesy a ID uživatelů, které se podílejí na doručování těchto zpráv.

Lokální řízení přístupu

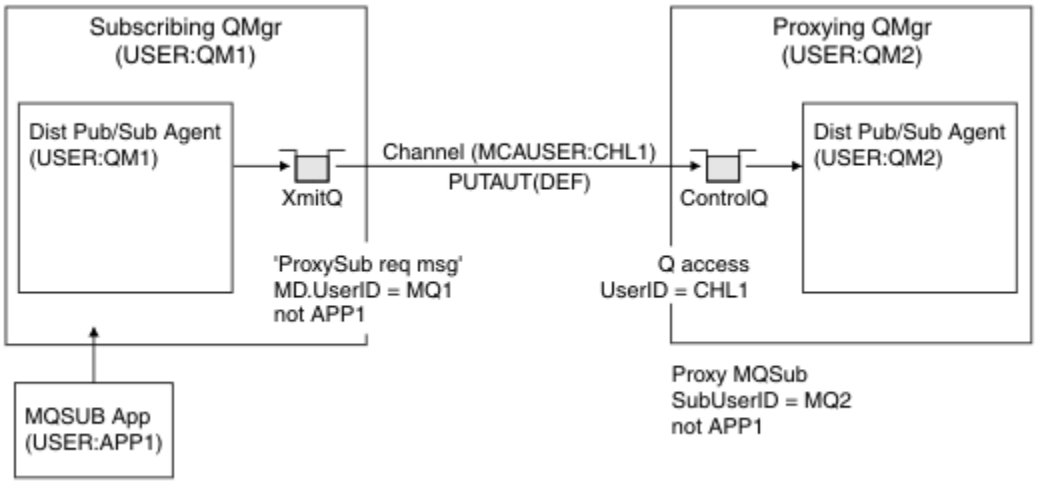
Přístup k tématům pro publikování a odběry je řízen lokálními definicemi zabezpečení a pravidly, které jsou popsány v tématu Zabezpečení publikování/odběru. V systému z/OSnení k zavedení řízení přístupu požadován žádný lokální objekt tématu. Pro řízení přístupu na jiných platformách není vyžadováno žádné lokální téma. Administrátoři se mohou rozhodnout použít řízení přístupu k objektům klastrovaných témat bez ohledu na to, zda již v klastru existují.

Systémoví administrátoři jsou odpovědní za řízení přístupu na svém lokálním systému. Musí důvěřovat administrátorům ostatních členů hierarchie nebo kolektivu klastru, aby byli odpovědní za jejich zásadu řízení přístupu. Vzhledem k tomu, že řízení přístupu je definováno pro každý samostatný počítač, je pravděpodobné, že bude tíživé, je-li zapotřebí kontrola na úrovni pokuty. Ve stromu témat nemusí být nutné definovat žádné řízení přístupu nebo řízení přístupu k vyšším objektům. Řízení přístupu na úrovni FGT lze definovat pro každou dílčí divizi oboru názvů témat.

Vytvoření proxy odběru

Důvěryhodnost organizace pro připojení správce front k vašemu správci front je potvrzena běžnými prostředky ověřování kanálu. Je-li tato důvěryhodná organizace také povolena k distribuovanému publikování/odběru, provede se kontrola oprávnění. Kontrola se provede, když kanál vloží zprávu do fronty distribuovaných publikování/odběru. Je-li například vložena zpráva do fronty `SYSTEM.INTER.QMGR.CONTROL` . ID uživatele pro kontrolu oprávnění fronty závisí na hodnotách typu PUTAUT přijímajícího kanálu. Příklad: ID uživatele kanálu, `MCAUSER`, kontext zprávy, v závislosti na hodnotě a platformě. Další informace o zabezpečení kanálu naleznete v tématu Zabezpečení kanálů.

Odběry proxy se provádějí s ID uživatele distribuovaného agenta publikování/odběru ve vzdáleném správci front. Například `QM2` v Obrázek 30 na stránce 494. Uživateli je poté snadno udělen přístup k lokálním profilům objektů tématu, protože ID uživatele je v systému definováno a neexistují tedy žádné konflikty domén.



Obrázek 30. Zabezpečení odběru proxy, provedení odběru

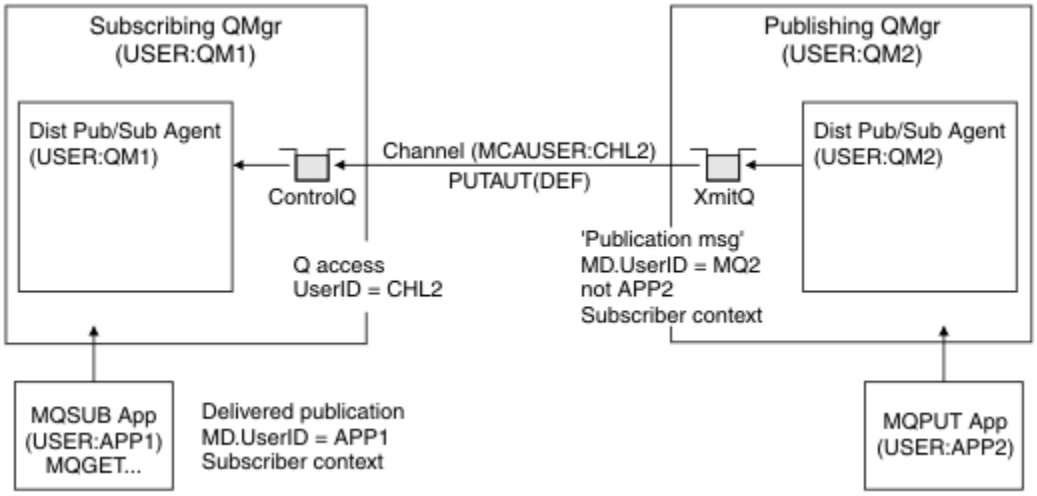
Odeslání vzdálených publikování

Je-li publikace vytvořena ve správci front publikování, je vytvořena kopie publikování pro každý odběr proxy. Kontext zkopírované publikace obsahuje kontext ID uživatele, který vytvořil odběr; `QM2` v produktu

Obrázek 31 na stránce 495. Proxy odběr se vytvoří s cílovou frontou, která je vzdálenou frontou, takže je zpráva publikování vyřešena do přenosové fronty.

Důvěryhodnost organizace pro připojení svého správce front QM2k jinému správci front QM1je potvrzena normálním ověřováním kanálu. Je-li tato důvěryhodná organizace poté povolena pro 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 parametru PUTAUT přijímajícího kanálu (například ID uživatele kanálu, MCAUSER, kontext zprávy a další informace v závislosti na hodnotě a platformě). Další informace o zabezpečení kanálu naleznete v tématu Zabezpečení kanálů.

Když se zpráva o publikování dostane do správce front odběru, provede se další příkaz MQPUT pro dané téma pod oprávněním správce front a kontext s touto zprávou je nahrazen kontextem každého z lokálních odběratelů, protože každá z nich má danou zprávu.



Obrázek 31. Zabezpečení odběru proxy, postoupení publikací

V systému, kde bylo zvažováno, že se týká zabezpečení, je pravděpodobné, že procesy distribuovaného publikování/odběru budou spuštěny pod ID uživatele ve skupině mqm , parametr MCAUSER na kanálu je prázdný (předvolba) a zprávy se doručí do různých systémových front podle potřeby. Nezabezpečený systém umožňuje snadné nastavení koncepce k demonstraci distribuovaného publikování/odběru.

V systému, kde je zabezpečení vážnější, se na tyto interní zprávy vztahují stejné ovládací prvky zabezpečení jako každá zpráva, která se přešla přes kanál.

Pokud je kanál nastaven s neprázdnou hodnotou MCAUSER a hodnotou PUTAUT určující, že MCAUSER musí být zkontrolována, pak musí mít MCAUSER udělen přístup k frontám SYSTEM.INTER.QMGR.* . Existuje-li více různých vzdálených správců front s kanály spuštěnými pod různými identifikátory MCAUSER , je třeba všem těmto ID uživatelů udělit přístup k frontám produktu SYSTEM.INTER.QMGR.* . Kanály spuštěné pod různými ID MCAUSER se mohou vyskytnout například v případě, že je v jednom správci front nakonfigurováno více hierarchických připojení.

Je-li kanál nastaven s hodnotou PUTAUT určující, že je použit kontext zprávy, pak je přístup k frontám SYSTEM.INTER.QMGR.* kontrolován na základě ID uživatele uvnitř interní zprávy. Protože všechny tyto zprávy jsou vloženy s ID uživatele distribuovaného agenta publikování/odběru ze správce front, který odesílá interní zprávu, nebo zprávu publikování (viz Obrázek 31 na stránce 495), není příliš velká sada ID uživatelů pro udělení přístupu k různým systémovým frontám (jeden pro vzdáleného správce front), pokud chcete tímto způsobem nastavit zabezpečení distribuovaného publikování/odběru. Stále má všechny stejné problémy, které zabezpečení kontextu kanálu vždy má, a to z různých domén ID uživatele a skutečnost, že ID uživatele ve zprávě nemusí být definováno v přijímajícím systému. Je to však naprosto přijatelný způsob, jak se v případě potřeby spustit.

z/OS Zabezpečení systémové fronty poskytuje seznam front a přístup, který je zapotřebí k bezpečnému nastavení distribuovaného prostředí publikování/odběr. Pokud dojde k selhání interních

zpráv nebo publikování kvůli narušení zabezpečení, kanál zapíše zprávu do protokolu normálním způsobem a zprávy lze odeslat do fronty nedoručených zpráv v souladu s normálním zpracováním chyb kanálu.

Všechny systémy zpráv mezi správci front pro účely distribuovaných publikování/odběru se spouštějí s použitím běžného zabezpečení kanálu.

Informace o omezení publikování a odběrů proxy na úrovni tématu naleznete v tématu Zabezpečení publikování/odběru.

Použití výchozích ID uživatelů s hierarchií správce front

Pokud máte hierarchii správců front spuštěných na různých platformách a používáte výchozí ID uživatelů, všimněte si, že tato výchozí ID uživatele se liší mezi platformami a nemusí být známá na cílové platformě. Výsledkem je, že správce front spuštěný na jedné platformě zamítá zprávy přijaté od správců front na jiných platformách s kódem příčiny `MQRC_NOT_AUTHORIZED`.

Chcete-li zabránit odmítnutí zpráv, je třeba přidat k výchozím ID uživatele, která se používají na jiných platformách, následující oprávnění:

- *PUT *GET oprávnění na SYSTEM.BROKER. fronty
- *PUB *SUB oprávnění na systému SYSTEM.BROKER. Témata
- *ADMCRT *ADMDLT *ADMCHG oprávnění na SYSTEM.BROKER.CONTROL.QUEUE fronta.

Výchozí jména uživatelů s hierarchií správce 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', je-li hierarchicky připojen ke správci front v produktu IBM i for Queue Managers na systémech z/OS, AIX, Linux, and Windows .

Pro správce front na platformách IBM i a z/OS vytvořte a udělte přístup k ID uživatele 'mqm', je-li hierarchicky připojen ke správci front v systému AIX, Linux, and Windows .

Vytvořte a udělte uživatelský přístup k ID uživatele adresního prostoru iniciátoru kanálu produktu z/OS , pokud je hierarchicky připojen ke správci front v produktu z/OS for Queue Managers v systému Multiplatforms.

ID uživatelů mohou rozlišovat malá a velká písmena. Původní správce front (pokud je v systému Multiplatforms) vynucuje, aby ID uživatele bylo vše velkými písmeny. Přijímající správce front (pokud je v systému AIX, Linux, and Windows) vynucuje, aby ID uživatele bylo vše malými písmeny. Proto musí být všechna ID uživatelů vytvořená na systémech AIX and Linux vytvořena ve svém formátu s malými písmeny. Byla-li instalována uživatelská procedura pro zprávy, vynucuje se ID uživatele velkými nebo malými písmeny. Je třeba věnovat pozornost tomu, jak procedura ukončení zprávy zpracovává ID uživatele.

Chcete-li se vyhnout potenciálním problémům s převodem ID uživatelů, postupujte takto:

- V systému AIX, Linux, and Windows se ujistěte, že ID uživatelů jsou uvedena malými písmeny.
- V systémech IBM i a z/OSzkontrolujte, zda jsou ID uživatelů zadána velkými písmeny.

Zabezpečení produktů IBM MQ Console a REST API

Zabezpečení pro IBM MQ Console a REST API se konfiguruje úpravou konfigurace mqweb serveru v souboru `mqwebuser.xml` .

Informace o této úloze

Můžete sledovat akce uživatele a monitorovat použití produktu IBM MQ Console a produktu REST API kontrolou souborů protokolu na webovém serveru mqweb.

Uživatelé IBM MQ Console a REST API mohou být ověřeni pomocí:

- Základní registr
- Registr LDAP
- Lokální registr OS
- SAF v systému z/OS
- Jakýkoli jiný typ registru podporovaný produktem WebSphere Liberty

Role lze přiřadit uživatelům produktu IBM MQ Console a uživatelům produktu REST API k určení, jakou úroveň přístupu mají být uděleny objektům produktu IBM MQ . Chcete-li například provádět systém zpráv, musí být uživatelům přiřazena role produktu `MQWebUser` . Další informace o dostupných rolích viz “Role na IBM MQ Console a REST API” na stránce 507.

Poté, co je uživateli přiřazena role, existuje řada metod, které lze použít k ověření uživatele. Pomocí produktu IBM MQ Consolese mohou uživatelé přihlásit pomocí jména uživatele a hesla nebo mohou používat ověření pomocí certifikátu klienta. S produktem REST APImohou uživatelé použít základní ověření HTTP, ověření založené na tokenech nebo ověření klientských certifikátů.

Postup

1. Definujte registr uživatelů pro ověření uživatelů a přiřaďte každému uživateli nebo skupině roli, která autorizuje uživatele a skupiny, aby mohli používat IBM MQ Console nebo REST API. Další informace naleznete zde: “Konfigurace uživatelů a rolí” na stránce 498
2. Zvolte, jak se uživatelé produktu IBM MQ Console ověřují s pomocí mqweb serveru. Stejnou metodu pro všechny uživatele nemusíte používat:
   - Nechat uživatele ověřit pomocí ověření tokenu. V takovém případě uživatel zadá ID uživatele a heslo na obrazovce produktu IBM MQ Console . Je vygenerován token LTPA, který umožňuje uživateli zůstat přihlášen a autorizován pro určitý časový interval. Pro použití této volby ověření není vyžadována žádná další konfigurace, ale můžete volitelně konfigurovat dobu vypršení platnosti tokenu LTPA. Další informace naleznete v tématu Konfigurace intervalu vypršení tokenu LTPA.
   - Nechte uživatele ověřovat certifikáty pomocí klientských certifikátů. V tomto případě uživatel nepoužije ID uživatele nebo heslo pro přihlášení k serveru IBM MQ Console, ale použije místo toho certifikát klienta. Další informace viz téma “Použití ověření klientského certifikátu s REST API a IBM MQ Console” na stránce 512.
3. Zvolte, jak se uživatelé produktu REST API ověřují s pomocí mqweb serveru. Stejnou metodu pro všechny uživatele nemusíte používat:
   - Nechte uživatele provést ověření pomocí základního ověření HTTP. V tomto případě je jméno uživatele a heslo zakódováno, ale není šifrováno a odesláno s každým požadavkem REST API na ověření a autorizaci uživatele pro tento požadavek. Má-li být toto ověření zabezpečené, je třeba použít zabezpečené připojení. To znamená, že musíte použít protokol HTTPS. Další informace viz téma “Použití základního ověření HTTP s produktem REST API” na stránce 516.
   - Nechat uživatele ověřit pomocí ověření tokenu. V tomto případě uživatel zadá ID uživatele a heslo do prostředku produktu REST API `login` pomocí metody HTTP POST. Je vygenerován token LTPA, který umožňuje uživateli zůstat přihlášen a autorizován pro určitý časový interval. Další informace viz téma “Použití ověření založeného na tokenech s rozhraním API služby REST” na stránce 517.

     Má-li být toto ověření zabezpečené, je třeba použít zabezpečené připojení. To znamená, že musíte použít protokol HTTPS. Pokud jste však povolili připojení HTTP, můžete povolit použití tokenu LTPA, který je vydán pro připojení HTTPS, k použití pro připojení HTTP. Další informace viz Konfigurace tokenu LTPA.
   - Nechte uživatele ověřovat certifikáty pomocí klientských certifikátů. V tomto případě uživatel nepoužije ID uživatele nebo heslo pro přihlášení k serveru REST API, ale použije místo toho

certifikát klienta. Další informace viz téma “Použití ověření klientského certifikátu s REST API a IBM MQ Console” na stránce 512.

4. Volitelné: Nakonfigurujte sdílení prostředků různého původu pro REST API.

   Ve výchozím nastavení webový prohlížeč nepovoluje skripty, jako je skript JavaScript, vyvolat REST API , když skript není ze stejného původu jako REST API. To znamená, že požadavky typu cross-origin nejsou povoleny. Sdílení CORS (Cross Origin Resource Sharing) můžete nakonfigurovat tak, aby bylo možné povolit požadavky na křížový původ ze zadaných adres URL. Další informace viz téma “Konfigurace CORS pro REST API” na stránce 519.

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 budou zpracovány pouze požadavky, které obsahují určitá záhlaví hostitele, a to pomocí IBM MQ Console a REST API. Další informace viz téma “Konfigurace ověření záhlaví hostitele pro IBM MQ Console a REST API” na stránce 520.

Konfigurace uživatelů a rolí

Chcete-li využít produkt IBM MQ Console nebo REST API, uživatelé se musí ověřit proti registru uživatelů definovanému na webovém serveru mqweb.

Informace o této úloze

Ověření uživatelé potřebují být členem jedné ze skupin, které autorizuje přístup k funkcím produktů IBM MQ Console a REST API. Standardně registr uživatelů neobsahuje žádné uživatele; je třeba jej přidat úpravou souboru `mqwebuser.xml` .

Když konfigurujete uživatele a skupiny, nejprve nakonfigurujete registr uživatelů pro ověření uživatelů a skupin proti. Tento registr uživatelů je sdílen mezi IBM MQ Console a REST API. Když konfigurujete role pro uživatele a skupiny, můžete řídit, zda mají uživatelé a skupiny přístup k serveru IBM MQ Console, REST APInebo oběma skupinám.

Jakmile nakonfigurujete registr uživatelů, nakonfigurujete role pro uživatele a skupiny, aby jim udělili oprávnění. K dispozici je několik rolí, včetně rolí specifických pro použití produktu REST API pro produkt Managed File Transfer. Každá role uděluje jinou úroveň přístupu. Další informace viz téma “Role na IBM MQ Console a REST API” na stránce 507.

Několik ukázkových souborů XML je k dispozici spolu s parametrem mqweb server, aby se konfigurace uživatelů a skupin zjednodušila. Uživatelé, kteří jsou obeznámeni s konfigurací zabezpečení v produktu WebSphere Liberty (WLP), mohou raději nepoužívat ukázky. WLP poskytuje další možnosti autorizace navíc k těm, 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` , prohlédněte si téma “Konfigurace základního registru pro produkty IBM MQ Console a REST API” na stránce 499.

- Nakonfigurujte uživatele a skupiny s registrem LDAP pomocí souboru `ldap_registry.xml` .

  Jména uživatelů a hesla v registru LDAP se používají pro 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 produkty IBM MQ Console a REST API” na stránce 503.

- 

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 nakonfigurovat lokální registr OS pomocí ukázkového souboru `local_os_registry.xml` , prohlédněte si téma "Konfigurace lokálního registru operačního systému pro IBM MQ Console a REST API" na stránce 502.

- z/OS

  Pomocí souboru `zos_saf_registry.xml` nakonfigurujte uživatele a skupiny pomocí rozhraní SAF (System Authorization Facility) v systému z/OS .

  RACF, nebo jiný produkt zabezpečení, profily se používají k udělení přístupu uživatelům a skupinám k rolím. Jména uživatelů a hesla v databázi RACF se používají k ověření a autorizaci uživatelů produktů IBM MQ Console a REST API.

  Chcete-li konfigurovat rozhraní SAF pomocí ukázkového souboru `zos_saf_registry.xml` , prohlédněte si téma "Konfigurace registru SAF pro IBM MQ Console a REST API" na stránce 505.
- Zakažte zabezpečení včetně možnosti přístupu k serveru IBM MQ Consolenebo produktu REST APIpomocí protokolu HTTPS pomocí souboru `no_security.xml` .

Jak pokračovat dále

Vyberte způsob ověření uživatelů:

IBM MQ Console Volby ověření

- Nechat uživatele ověřit pomocí ověření tokenu. V takovém případě uživatel zadá ID uživatele a heslo na obrazovce produktu IBM MQ Console . Je vygenerován token LTPA, který umožňuje uživateli zůstat přihlášen a autorizován pro určitý časový interval. Pro použití této volby ověření není vyžadována žádná další konfigurace, ale můžete volitelně nakonfigurovat interval vypršení platnosti tokenu LTPA. Další informace naleznete v tématu Konfigurace intervalu vypršení tokenu LTPA.
- Nechte uživatele ověřovat certifikáty pomocí klientských certifikátů. V tomto případě uživatel nepoužije ID uživatele nebo heslo pro přihlášení k serveru IBM MQ Console, ale použije místo toho certifikát klienta. Další informace viz téma "Použití ověření klientského certifikátu s REST API a IBM MQ Console" na stránce 512.

REST API Volby ověření

- Nechte uživatele provést ověření pomocí základního ověření HTTP. V tomto případě je jméno uživatele a heslo zakódováno, ale není šifrováno a odesláno s každým požadavkem REST API na ověření a autorizaci uživatele pro tento požadavek. Má-li být toto ověření zabezpečené, je třeba použít zabezpečené připojení. To znamená, že musíte použít protokol HTTPS. Další informace viz téma "Použití základního ověření HTTP s produktem REST API" na stránce 516.
- Nechat uživatele ověřit pomocí ověření tokenu. V tomto případě uživatel zadá ID uživatele a heslo do prostředku produktu REST API `login` pomocí metody HTTP POST. Je vygenerován token LTPA, který umožňuje uživateli zůstat přihlášen a autorizován pro určitý časový interval. Další informace viz téma "Použití ověření založeného na tokenech s rozhraním API služby REST" na stránce 517. Interval vypršení platnosti pro token LTPA můžete nakonfigurovat. Další informace viz Konfigurace tokenu LTPA.
- Nechte uživatele ověřovat certifikáty pomocí klientských certifikátů. V tomto případě uživatel nepoužije ID uživatele nebo heslo pro přihlášení k serveru REST API, ale použije místo toho certifikát klienta. Další informace viz téma "Použití ověření klientského certifikátu s REST API a IBM MQ Console" na stránce 512.

Konfigurace základního registru pro produkty IBM MQ Console a REST API

Základní registr lze konfigurovat v rámci 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 IBM MQ Console a REST API, a určuje kontext zabezpečení, který se použije při pokusu o povolení operace. Tyto role musíte pochopit, než budete konfigurovat základní registr. Další informace o každé z rolí naleznete v tématu “Role na IBM MQ Console a REST API” na stránce 507.
- Chcete-li dokončit tuto úlohu, musíte být uživatel s dostatečnými oprávněními pro úpravu souboru `mqwebuser.xml` :
  - z/OS V systému z/OSmusíte mít přístup pro zápis k souboru `mqwebuser.xml` .
  - Multi U všech ostatních operačních systémů musíte být privilegovaný uživatel.

Postup

1. Zkopírujte ukázkový soubor XML `basic_registry.xml` z jedné z následujících cest:
   - 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 produktu IBM MQ for z/OS UNIX System Services Components .
2. Umístěte ukázkový soubor do odpovídajícího adresáře:
   - ALW

     V systému AIX, Linux, and Windows: *MQ_DATA_PATH*`/web/installations/`*`installationName`*`/servers/mqweb`
   - z/OS

     V systému z/OS: *`WLP_user_directory`*`/servers/mqweb`

     kde *WLP_user_directory* je adresář, který byl zadán při spuštění skriptu **crtmqweb** za účelem vytvoření definice mqweb serveru.
3. Volitelné: Pokud jste změnili jakékoli nastavení konfigurace v produktu `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 do značek produktu **basicRegistry** .

   Mějte na paměti, že každý uživatel s rolí `MQWebUser` může provádět pouze operace, které má uděleno ID uživatele 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 případu, nebo mapování mezi ID uživatele může selhat.

   Další informace o konfiguraci základních registrů uživatelů najdete v tématu Konfigurace základního registru uživatelů pro Liberty v dokumentaci produktu WebSphere Liberty .
6. Přiřaďte role uživatelům a skupinám úpravou souboru `mqwebuser.xml` :

   K dispozici je několik rolí, které autorizují uživatele a skupiny k použití produktu IBM MQ Consolea produktu REST API. Každá role uděluje jinou úroveň přístupu. Další informace viz téma “Role na IBM MQ Console a REST API” na stránce 507.
   - Chcete-li přiřadit role a udělit přístup k produktu IBM MQ Console, přidejte uživatele a skupiny mezi příslušné značky produktu **security-role** do značek produktu **<enterpriseApplication id="com.ibm.mq.console">** .

- Chcete-li přiřadit role a udělit přístup k produktu REST API, přidejte uživatele a skupiny mezi příslušné značky produktu **security-role** do značek produktu **<enterpriseApplication id="com.ibm.mq.rest">** .

  Nápovědu k formátu informací o uživateli a skupině ve značkách **security-role** naleznete v příkladech.

7. Pokud jste zadali hesla pro uživatele v produktu `mqwebuser.xml`, měli byste tato hesla zakódovat, aby byla zajištěna bezpečněji, pomocí příkazu **securityUtility encoding** poskytovaného produktem WebSphere Liberty. Další informace viz Příkaz Liberty: PříkazsecurityUtility v dokumentaci produktu WebSphere Liberty .

Příklad

V následujícím příkladu je skupině `MQWebAdminGroup` udělen přístup k IBM MQ Console s rolí `MQWebAdmin`. Uživateli, `reader`, je udělen přístup k roli `MQWebAdminRO`a uživateli `guest` je udělen přístup k roli `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 uživateli `reader` a `guest` udělen přístup k serveru IBM MQ Console. Uživateli `user` je udělen přístup k REST APIa všem uživatelům v rámci skupiny `MQAdmin` je udělen přístup k IBM MQ Console a REST API. Uživateli `mftadmin` je udělen přístup k 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

Vyberte způsob ověření uživatelů:

IBM MQ Console Volby ověření

- Nechat uživatele ověřit pomocí ověření tokenu. V takovém případě uživatel zadá ID uživatele a heslo na obrazovce produktu IBM MQ Console . Je vygenerován token LTPA, který umožňuje

uživateli zůstat přihlášen a autorizován pro určitý časový interval. Pro použití této volby ověření není vyžadována žádná další konfigurace, ale můžete volitelně nakonfigurovat interval vypršení platnosti tokenu LTPA. Další informace naleznete v tématu Konfigurace intervalu vypršení tokenu LTPA.

- Nechte uživatele ověřovat certifikáty pomocí klientských certifikátů. V tomto případě uživatel nepoužije ID uživatele nebo heslo pro přihlášení k serveru IBM MQ Console, ale použije místo toho certifikát klienta. Další informace viz téma “Použití ověření klientského certifikátu s REST API a IBM MQ Console” na stránce 512.

REST API Volby ověření

- Nechte uživatele provést ověření pomocí základního ověření HTTP. V tomto případě je jméno uživatele a heslo zakódováno, ale není šifrováno a odesláno s každým požadavkem REST API na ověření a autorizaci uživatele pro tento požadavek. Má-li být toto ověření zabezpečené, je třeba použít zabezpečené připojení. To znamená, že musíte použít protokol HTTPS. Další informace viz téma “Použití základního ověření HTTP s produktem REST API” na stránce 516.
- Nechat uživatele ověřit pomocí ověření tokenu. V tomto případě uživatel zadá ID uživatele a heslo do prostředku produktu REST API `login` pomocí metody HTTP POST. Je vygenerován token LTPA, který umožňuje uživateli zůstat přihlášen a autorizován pro určitý časový interval. Další informace viz téma “Použití ověření založeného na tokenech s rozhraním API služby REST” na stránce 517. Interval vypršení platnosti pro token LTPA můžete nakonfigurovat. Další informace viz Konfigurace tokenu LTPA.
- Nechte uživatele ověřovat certifikáty pomocí klientských certifikátů. V tomto případě uživatel nepoužije ID uživatele nebo heslo pro přihlášení k serveru REST API, ale použije místo toho certifikát klienta. Další informace viz téma “Použití ověření klientského certifikátu s REST API a IBM MQ Console” na stránce 512.

ALW Konfigurace lokálního registru operačního systému pro IBM MQ Console a REST API

Registr lokálního operačního systému je možné konfigurovat v rámci souboru `mqwebuser.xml` . Jména uživatelů a hesla na lokálním operačním systému se používají k ověření a autorizaci uživatelů IBM MQ Console a REST API.

Než začnete

- Pro ověření klientského certifikátu s funkcí lokálního ověření operačního systému je identita uživatele obecný název (CN) z rozlišujícího názvu (DN) certifikátu klienta. Pokud totožnost uživatele neexistuje jako uživatel operačního systému, přihlášení k certifikátu klienta selže a náhradní ověření na základě hesla.
- Chcete-li dokončit tuto úlohu, musíte být privilegovaný uživatel.

Informace o této úloze

Při použití registru lokálního operačního systému jsou uživatelé a skupiny automaticky přiřazeni k roli:

- Každý uživatel, který je součástí skupiny 'mqm', nebo skupina 'QMQMADM' na systému IBM i, má udělenou roli MQWebAdmin a MFTWebAdmin .
- Všem ostatním uživatelům je udělena role MQWebUser .

Další informace o těchto rolích najdete v tématu “Role na IBM MQ Console a REST API” na stránce 507.

Lokální registr operačního systému lze použít pouze v produktu AIX, Linux, and Windows. V produktu z/OS je k dispozici ekvivalentní funkce nakonfigurováním registru SAF. Další informace viz téma “Konfigurace registru SAF pro IBM MQ Console a REST API” na stránce 505.

Postup

1. Zkopírujte ukázkový soubor XML `local_os_registry.xml` z následující cesty:

MQ_INSTALLATION_PATH/web/mq/samp/configuration

2. Umístěte ukázkový soubor do následujícího adresáře:
   MQ_DATA_PATH/web/installations/*installationName*/servers/mqweb
3. Volitelné: Pokud jste změnili jakékoli nastavení konfigurace v produktu mqwebuser.xml, zkopírujte je do ukázkového souboru.
4. Odstraňte existující soubor mqwebuser.xml a přejmenujte ukázkový soubor na mqwebuser.xml.

Jak pokračovat dále

Vyberte způsob ověření uživatelů:

IBM MQ Console Volby ověření

- Nechat uživatele ověřit pomocí ověření tokenu. V takovém případě uživatel zadá ID uživatele a heslo na obrazovce produktu IBM MQ Console . Je vygenerován token LTPA, který umožňuje uživateli zůstat přihlášen a autorizován pro určitý časový interval. Pro použití této volby ověření není vyžadována žádná další konfigurace, ale můžete volitelně nakonfigurovat interval vypršení platnosti tokenu LTPA. Další informace naleznete v tématu Konfigurace intervalu vypršení tokenu LTPA.
- Nechte uživatele ověřovat certifikáty pomocí klientských certifikátů. V tomto případě uživatel nepoužije ID uživatele nebo heslo pro přihlášení k serveru IBM MQ Console, ale použije místo toho certifikát klienta. Další informace viz téma “Použití ověření klientského certifikátu s REST API a IBM MQ Console” na stránce 512.

REST API Volby ověření

- Nechte uživatele provést ověření pomocí základního ověření HTTP. V tomto případě je jméno uživatele a heslo zakódováno, ale není šifrováno a odesláno s každým požadavkem REST API na ověření a autorizaci uživatele pro tento požadavek. Má-li být toto ověření zabezpečené, je třeba použít zabezpečené připojení. To znamená, že musíte použít protokol HTTPS. Další informace viz téma “Použití základního ověření HTTP s produktem REST API” na stránce 516.
- Nechat uživatele ověřit pomocí ověření tokenu. V tomto případě uživatel zadá ID uživatele a heslo do prostředku produktu REST API login pomocí metody HTTP POST. Je vygenerován token LTPA, který umožňuje uživateli zůstat přihlášen a autorizován pro určitý časový interval. Další informace viz téma “Použití ověření založeného na tokenech s rozhraním API služby REST” na stránce 517. Interval vypršení platnosti pro token LTPA můžete nakonfigurovat. Další informace viz Konfigurace tokenu LTPA.
- Nechte uživatele ověřovat certifikáty pomocí klientských certifikátů. V tomto případě uživatel nepoužije ID uživatele nebo heslo pro přihlášení k serveru REST API, ale použije místo toho certifikát klienta. Další informace viz téma “Použití ověření klientského certifikátu s REST API a IBM MQ Console” na stránce 512.

Konfigurace registru LDAP pro produkty IBM MQ Console a REST API

Registr LDAP můžete nakonfigurovat v rámci 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 IBM MQ Console a REST API, a určuje kontext zabezpečení, který se použije při pokusu o povolení operace. Tyto role musíte pochopit, než budete moci nakonfigurovat registr. Další informace o každé z rolí naleznete v tématu “Role na IBM MQ Console a REST API” na stránce 507.

  Mějte na paměti, že každý uživatel s rolí MQWebUser může provádět pouze operace, které má uděleno ID uživatele 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 případu, nebo mapování mezi ID uživatele může selhat.

- Chcete-li dokončit tuto úlohu, musíte být uživatel s dostatečnými oprávněními pro úpravu souboru `mqwebuser.xml` :
  - z/OS V systému z/OSmusíte mít přístup pro zápis k souboru `mqwebuser.xml` .
  - Multi U všech ostatních operačních systémů musíte být privilegovaný uživatel.

Postup

1. Zkopírujte ukázkový soubor XML `ldap_registry.xml` z jedné z následujících cest:
   - 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 produktu IBM MQ for z/OS UNIX System Services Components .
2. Umístěte ukázkový soubor do odpovídajícího adresáře:
   - ALW

     V systému AIX, Linux, and Windows: *MQ_DATA_PATH*`/web/installations/`*installationName*`/servers/mqweb`
   - z/OS

     V systému z/OS: *WLP_user_directory*`/servers/mqweb`

     kde *WLP_user_directory* je adresář, který byl zadán při spuštění skriptu **crtmqweb** za účelem vytvoření definice mqweb serveru.
3. Volitelné: Pokud jste změnili jakékoli nastavení konfigurace v produktu `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` , abyste změnili nastavení registru LDAP v rámci značek **ldapRegistry** a **idsLdapFilterProperties** .

   Další informace o konfiguraci registrů LDAP najdete v tématu Konfigurace registrů uživatelů LDAP v Liberty v dokumentaci produktu WebSphere Liberty .
6. Přiřaďte role uživatelům a skupinám úpravou souboru `mqwebuser.xml` :

   K dispozici je několik rolí, které autorizují uživatele a skupiny k použití produktu IBM MQ Consolea produktu REST API. Každá role uděluje jinou úroveň přístupu. Další informace viz téma “Role na IBM MQ Console a REST API” na stránce 507.
   - Chcete-li přiřadit role a udělit přístup k produktu IBM MQ Console, přidejte uživatele a skupiny mezi příslušné značky produktu **security-role** do značek produktu **<enterpriseApplication id="com.ibm.mq.console">** .
   - Chcete-li přiřadit role a udělit přístup k produktu REST API, přidejte uživatele a skupiny mezi příslušné značky produktu **security-role** do značek produktu **<enterpriseApplication id="com.ibm.mq.rest">** .

Jak pokračovat dále

Vyberte způsob ověření uživatelů:

IBM MQ Console Volby ověření

- Nechat uživatele ověřit pomocí ověření tokenu. V takovém případě uživatel zadá ID uživatele a heslo na obrazovce produktu IBM MQ Console . Je vygenerován token LTPA, který umožňuje uživateli zůstat přihlášen a autorizován pro určitý časový interval. Pro použití této volby ověření není vyžadována žádná další konfigurace, ale můžete volitelně nakonfigurovat interval vypršení platnosti tokenu LTPA. Další informace naleznete v tématu Konfigurace intervalu vypršení tokenu LTPA.

- Nechte uživatele ověřovat certifikáty pomocí klientských certifikátů. V tomto případě uživatel nepoužije ID uživatele nebo heslo pro přihlášení k serveru IBM MQ Console, ale použije místo toho certifikát klienta. Další informace viz téma “Použití ověření klientského certifikátu s REST API a IBM MQ Console” na stránce 512.

REST API Volby ověření

- Nechte uživatele provést ověření pomocí základního ověření HTTP. V tomto případě je jméno uživatele a heslo zakódováno, ale není šifrováno a odesláno s každým požadavkem REST API na ověření a autorizaci uživatele pro tento požadavek. Má-li být toto ověření zabezpečené, je třeba použít zabezpečené připojení. To znamená, že musíte použít protokol HTTPS. Další informace viz téma “Použití základního ověření HTTP s produktem REST API” na stránce 516.
- Nechat uživatele ověřit pomocí ověření tokenu. V tomto případě uživatel zadá ID uživatele a heslo do prostředku produktu REST API `login` pomocí metody HTTP POST. Je vygenerován token LTPA, který umožňuje uživateli zůstat přihlášen a autorizován pro určitý časový interval. Další informace viz téma “Použití ověření založeného na tokenech s rozhraním API služby REST” na stránce 517. Interval vypršení platnosti pro token LTPA můžete nakonfigurovat. Další informace viz Konfigurace tokenu LTPA.
- Nechte uživatele ověřovat certifikáty pomocí klientských certifikátů. V tomto případě uživatel nepoužije ID uživatele nebo heslo pro přihlášení k serveru REST API, ale použije místo toho certifikát klienta. Další informace viz téma “Použití ověření klientského certifikátu s REST API a IBM MQ Console” na stránce 512.

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 507.
- 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: V9.2.0.25 V produktu IBM MQ 9.2.0 Fix Pack 25byl 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 MQ Console na z/OS upgraduje na úroveň, která se dodává WebSphere Liberty Profile 22.0.0.12 nebo novější: tj. z IBM MQ 9.2.0 CSU 8. 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 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.jclzměňte 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 506.
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 506. 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 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 506. 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 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 506.

```
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 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 506. Další informace o rolích viz “Role na IBM MQ Console a REST API” na stránce 507.

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 506.

```
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

Vyberte způsob ověření uživatelů:

IBM MQ Console Volby ověření

- Nechat uživatele ověřit pomocí ověření tokenu. V takovém případě uživatel zadá ID uživatele a heslo na obrazovce produktu IBM MQ Console . Je vygenerován token LTPA, který umožňuje uživateli zůstat přihlášen a autorizován pro určitý časový interval. Pro použití této volby ověření není vyžadována žádná další konfigurace, ale můžete volitelně nakonfigurovat interval vypršení platnosti tokenu LTPA. Další informace naleznete v tématu Konfigurace intervalu vypršení tokenu LTPA.
- Nechte uživatele ověřovat certifikáty pomocí klientských certifikátů. V tomto případě uživatel nepoužije ID uživatele nebo heslo pro přihlášení k serveru IBM MQ Console, ale použije místo toho certifikát klienta. Další informace viz téma “Použití ověření klientského certifikátu s REST API a IBM MQ Console” na stránce 512.

REST API Volby ověření

- Nechte uživatele provést ověření pomocí základního ověření HTTP. V tomto případě je jméno uživatele a heslo zakódováno, ale není šifrováno a odesláno s každým požadavkem REST API na ověření a autorizaci uživatele pro tento požadavek. Má-li být toto ověření zabezpečené, je třeba použít zabezpečené připojení. To znamená, že musíte použít protokol HTTPS. Další informace viz téma “Použití základního ověření HTTP s produktem REST API” na stránce 516.
- Nechat uživatele ověřit pomocí ověření tokenu. V tomto případě uživatel zadá ID uživatele a heslo do prostředku produktu REST API `login` pomocí metody HTTP POST. Je vygenerován token LTPA, který umožňuje uživateli zůstat přihlášen a autorizován pro určitý časový interval. Další informace viz téma “Použití ověření založeného na tokenech s rozhraním API služby REST” na stránce 517. Interval vypršení platnosti pro token LTPA můžete nakonfigurovat. Další informace viz Konfigurace tokenu LTPA.
- Nechte uživatele ověřovat certifikáty pomocí klientských certifikátů. V tomto případě uživatel nepoužije ID uživatele nebo heslo pro přihlášení k serveru REST API, ale použije místo toho certifikát klienta. Další informace viz téma “Použití ověření klientského certifikátu s REST API a IBM MQ Console” na stránce 512.

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 508 .

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 498.

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 poskytovaného produktem IBM MQ Console ve vašem prohlížeči

Produkt IBM MQ Console můžete nakonfigurovat tak, aby prezentujete svůj vlastní certifikát podepsaný certifikační autoritou (CA) pro účely ověření. Tím se odstraní varování certifikátu podepsaného držitelem, které vám předkládá webový prohlížeč při přístupu ke konzole IBM MQ Console

Než začnete

Konfigurujte uživatele, skupiny a role, abyste byli autorizováni používat produkt IBM MQ Console. Další informace viz téma "Konfigurace uživatelů a rolí" na stránce 498.

Informace o této úloze

Zabezpečení konzoly je poskytováno produktem IBM WebSphere Application Server Liberty používaným při instalaci produktu IBM MQ .

Chcete-li změnit certifikát, který je prezentován na vašem prohlížeči tímto serverem, je třeba:

1. Přidejte certifikát, který chcete prezentovat, do úložiště klíčů webového serveru.
2. Označte certifikát.
3. Chcete-li vypnout výchozí konfiguraci zabezpečení, upravte soubor `mqwebuser.xml` .
4. Zapněte si vlastní konfiguraci zabezpečení v souboru `mqwebuser.xml` a zadejte certifikát, který chcete prezentovat.

Procedura předpokládá, že jste:

- Pomocí systému AIX, Linux, and Windows .
- Oprávněný uživatel.

Notes:

- Následující příklad vytváří a používá certifikát podepsaný svým držitelem pomocí příkazů zadaných na počítači se systémem Linux ; to je **ls**, nikoli **dir** používaný na počítači s Windows .
- To vám ukáže koncept, ale neodebere varování prohlížeče.
- Chcete-li odebrat varování prohlížeče, musíte poskytnout certifikát podepsaný CA.

Postup

1. Je-li server Liberty spuštěn, zastavte server zadáním příkazu **endmqweb** na příkazový řádek.
2. Přidejte svůj certifikát do úložiště klíčů, které používá aplikační server produktu Liberty , aby mohl tento certifikát nalézt a prezentovat jej ve webovém prohlížeči.
   a) Přesuňte se do umístění úložiště klíčů zadáním následujícího příkazu a vypište výstup:

```
cd /var/mqm/web/installations/Installation1/servers/mqweb/resources/security
ls
```

   Například se zobrazí následující výstup, který zobrazuje 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 je přidán do produktu `key.jks` s heslem `password`, zadejte tento příkaz:

```
runmqckm -cert -create -db key.jks -pw password -dn
"cn=QueueManager,o=IBM,c=UK" -label myowncertificate
```

   Parametr **-dn** umožňuje zadat hodnoty, které se zobrazí 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 byl certifikát 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.

   Okomentujte následující řádek přidáním `<!--` na začátek řádku kódu a `-->` až po konec řádku kódu:

```
<!--
<sslDefault sslRef="mqDefaultSSLConfig"/>
-->
```

   c) Povolte a zadejte vlastní konfiguraci.

   Chcete-li to provést, proveďte následující proceduru:

   i) Odkomentujte následující řádky kódu odstraněním znaku `<!--` ze začátku bloku kódu a `-->` 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 ukládání svých osobních certifikátů.

iii) **Označte jako komentář druhý řádek bloku kódu**, protože tato řádka uvádí úložiště údajů o důvěryhodnosti, kde konzola bude hledat certifikáty klienta. Jelikož používáte ověření tokenu, nevytvořili jste úložiště údajů o důvěryhodnosti a zanechání řádku kódu by způsobilo chybu při spuštění konzoly.

iv) **Změňte hodnotu serverKeyAlias= "default" na serverKeyAlias= "myowncertificate"** ve třetím řádku bloku kódu a ponechejte vše ostatní stejné.

v) **Neměňte poslední řádek** bloku kódu, protože to říká serveru, že má používat právě zadanou konfiguraci.

Blok kódu nyní vypadá takto:

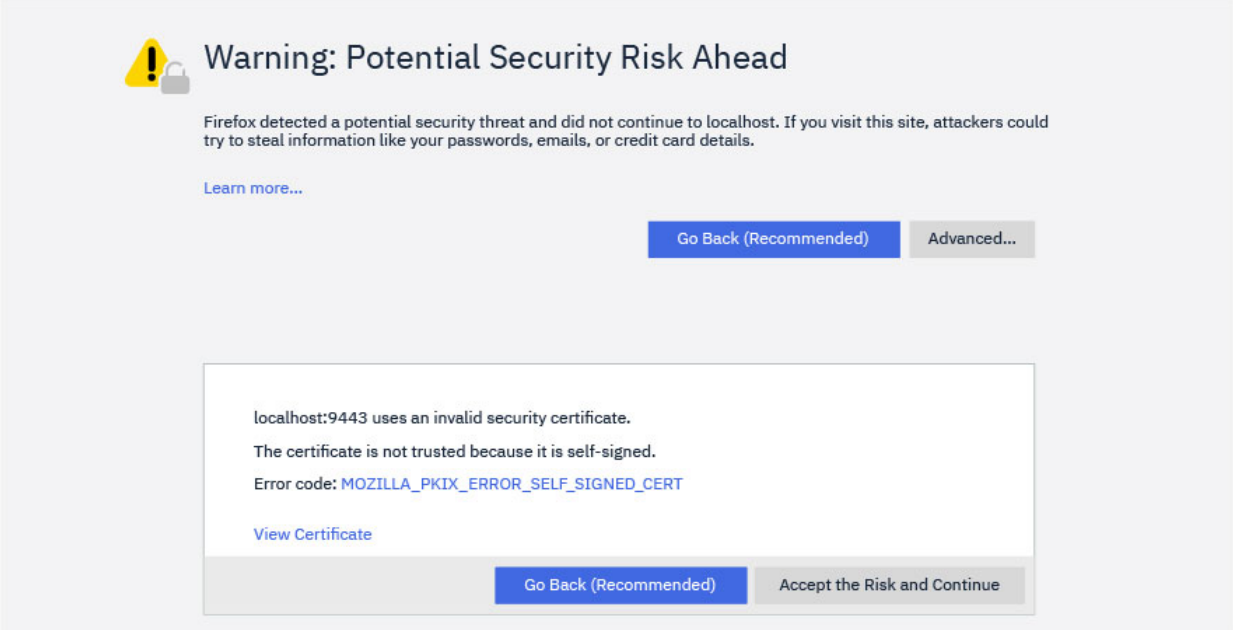
```
<keyStore id="defaultKeyStore" location="key.jks" type="JKS" password="password"/>
<!-- Commenting out the defaultTrustStore as otherwise we get errors (viewable in the messages.log file
in the logs folder) j
<keyStore id="defaultTrustStore" location="trust.jks" type="JKS" password="password"/>
-->
<ssl id="thisSSLConfig" clientAuthenticationSupported="true" keyStoreRef="defaultKeyStore"
serverKeyAlias="myowncertificate" trustStoreRef="defaultTrustStore" sslProtocol="TLSv1.2"/>
<sslDefault sslRef="thisSSLConfig"/>
```

4. Restartujte webový server pomocí příkazu **strmqweb** .

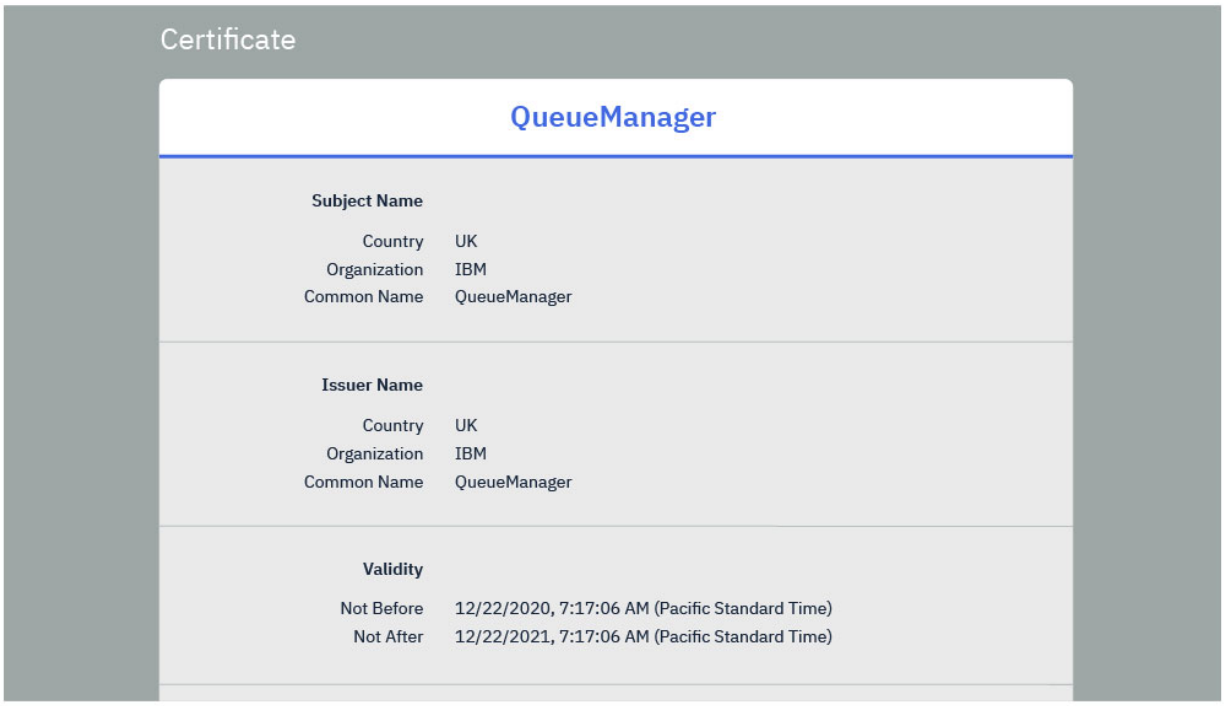
Výsledky

Po spuštění webového serveru přejděte k produktu IBM MQ Console a aktualizujte. Používáte-li certifikát podepsaný držitelem, který jste vytvořili pomocí postupu popsaného v předchozích krocích v krocích “2” na stránce 510 a “3” na stránce 510, uvidíte varování zabezpečení.

Všimněte si, že formát tohoto varování závisí na prohlížeči, který používáte.



Pokud klepnete na volbu **Zobrazit certifikát**, uvidíte, že má podrobnosti, které jste zadali při vytváření certifikátu v kroku “2.b” na stránce 510, na příznaku **-dn** .



Pokud však používáte certifikát podepsaný certifikační autoritou, který váš prohlížeč důvěřuje, který jste přidali, zadáním následujícího příkazu:

```
runmqckm -cert -add -db key.jks -pw password -label myCACertificate
```

kde `myCACertificate` je cesta k souboru s certifikátem CA, který jste přijali přímo na přihlašovací stránku.

Upozornění: Pokud používáte certifikát podepsaný CA a tento certifikát CA je součástí řetězu certifikátů, musíte přidat všechny certifikáty do řetězce počínaje kořenovým certifikátem CA. Další informace viz “Přidání certifikátu CA nebo veřejné části certifikátu podepsaného (svým držitelem) do úložiště klíčů v systému AIX, Linux, and Windows” na stránce 297.

ALW Použití ověření klientského certifikátu s REST API a IBM MQ Console

Klientské certifikáty můžete mapovat na činitele za účelem ověření uživatelů IBM MQ Console a REST API .

Než začnete

- Konfigurujte uživatele, skupiny a role, abyste byli autorizováni používat produkty IBM MQ Console a REST API. Další informace viz téma “Konfigurace uživatelů a rolí” na stránce 498.
- Když použijete produkt REST API, můžete se dotázat na pověření aktuálního uživatele pomocí metody HTTP GET na prostředku `login` , který poskytuje certifikát klienta k ověření požadavku. Tento požadavek vrátí informace o jménu uživatele a o rolích, které je uživatel přiřazen. Další informace viz GET `/login`.
- Při mapování klientských certifikátů na činitele za účelem ověření uživatelů se rozlišující název certifikátu klienta používá k porovnání s uživateli v konfigurovaném registru uživatelů:
  - Pro základní registr se shoduje obecný název (CN) proti uživateli. Například `CN=Fred, O=IBM, C=GB` se shoduje se jménem uživatele `Fred`.

– V případě registru LDAP je při výchozím nastavení úplný rozlišující název porovnáván s protokolem LDAP. Můžete nastavit filtry a mapování pro přizpůsobení porovnávání. Další informace viz téma Liberty :Režim mapování certifikátu LDAP v dokumentaci produktu WebSphere Liberty .

Informace o této úloze

Když se uživatel autentizuje pomocí certifikátu klienta, použije se místo jména uživatele a hesla. V případě REST APIje certifikát klienta poskytnut s každým požadavkem REST k ověření uživatele. Pokud se uživatel přihlašuje k certifikátu IBM MQ Console, uživatel nemůže být poté odhlášen.

Procedura předpokládá následující informace:

- Že váš soubor `mqwebuser.xml` je založen na jednom 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 konfigurovat ověření klientských certifikátů pomocí klíčového řetězce RACF na systému z/OS, postupujte podle pokynů v části “Konfigurace TLS pro REST API a IBM MQ Console na z/OS” na stránce 524.

Poznámka: Následující postup popisuje kroky nezbytné k použití klientských certifikátů s produkty IBM MQ Console a REST API. Pro pohodlí vývojářů kroky podrobně popisují, jak vytvářet a používat certifikáty podepsané sebou samým. Avšak pro produkci použijte certifikáty, které jsou získány od certifikační autority.

Postup

1. Zadáním příkazu **strmqweb** na příkazový řádek spusťte program mqweb.
2. Vytvořte certifikát klienta:
   a) Vytvořte úložiště klíčů PKCS#12 :
      i) Otevřete nástroj IBM Key Management zadáním příkazu **strmqikm** na příkazový řádek.
      ii) V nabídce **Soubor databáze klíčů** v nástroji Správa klíčů IBM klepněte na volbu **Nový**.
      iii) Vyberte položku **PKCS12** ze seznamu **Typ databáze klíčů** .
      iv) Vyberte umístění, do kterého chcete uložit úložiště klíčů, a do pole **Název souboru** zadejte příslušný název. Například `user.p12`
      v) Když jste vyzváni, nastavte heslo.
   b) Vytvořte certifikát, a to buď vytvořením certifikátu podepsaného sebou samým, nebo získáním certifikátu od certifikační autority:
      - Vytvořte certifikát podepsaný (svým) držitelem:
        i) Klepněte na volbu **Nový samostatně podepsaný**.
        ii) Do pole **Jmenovka klíče** zadejte `user` .
        iii) Používáte-li základní registr uživatelů, zadejte do pole **Obecné jméno** jméno uživatele z vašeho registru uživatelů. 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) rozlišujícího názvu (DN):
        i) Vyžádejte si nový certifikát. V nabídce **Vytvořit** klepněte na **Nový požadavek na certifikát**.
        ii) Do pole **Jmenovka klíče** zadejte jmenovku certifikátu.

iii) Používáte-li základní registr uživatelů, zadejte do pole **Obecné jméno** jméno uživatele, pro kterého je certifikát určen.

Pokud používáte lokální registr OS, pole **Obecné jméno** 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 toho, co je relevantní.

v) Vyberte, kam chcete uložit žádost o certifikát, a název souboru pro žádost o certifikát, poté klepněte na tlačítko **OK**.

vi) Odešlete soubor požadavku na certifikát certifikační autoritě (CA).

vii) Když máte certifikát od CA, otevřete nástroj IBM Key Management zadáním příkazu **strmqikm** na příkazový řádek.

viii) V nabídce **Soubor databáze klíčů** v nástroji IBM Key Management klepněte na **Otevřít**.

ix) Vyberte úložiště klíčů PKCS#12 , které zadržuje 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 IBM Key Management zadáním příkazu **strmqikm** na příkazový řádek.
   b) V nabídce **Soubor databáze klíčů** v nástroji IBM Key Management klepněte na **Otevřít**.
   c) Vyberte úložiště klíčů PKCS#12 , které zadržuje certifikát klienta. Například: `user.p12`
   d) Vyberte certifikát klienta ze seznamu certifikátů v nástroji IBM Key Management.
   e) Klepněte na tlačítko **Extrahovat certifikát**.
   f) Vyberte umístění, kam se má uložit certifikát, a do pole **Název souboru certifikátu** zadejte odpovídající název souboru. Například `user.arm`.
4. Importujte veřejnou část certifikátu klienta do úložiště údajů o důvěryhodnosti serveru mqWeb jako certifikát podepsaného, aby mohl server ověřit certifikát klienta:
   a) Vytvořte úložiště klíčů produktu `trust.jks` pro použití na webovém serveru mqweb, pokud dosud neexistuje:
      i) V nabídce **Soubor databáze klíčů** v nástroji Správa klíčů IBM klepněte na volbu **Nový**.
      ii) Vyberte **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 měl již obsahovat soubor `key.jks` . Pokud již soubor `trust.jks` existuje, pak jej otevřete a nepřepíše jej.

      iv) Do pole **Název souboru** zadejte `trust.jks` .
      v) Když jste vyzváni, nastavte heslo.
   b) Z rozevírací nabídky vyberte volbu **Certifikáty podepsaného**.
   c) Klepněte na tlačítko **Přidat**.
   d) Vyberte příslušný soubor raménka a klepněte na tlačítko **OK**. Vyberte například volbu `user.arm`.
   e) Zadejte jmenovku certifikátu.
5. Změňte heslo úložiště klíčů serveru mqweb:
   a) V nabídce **Soubor databáze klíčů** klepněte na volbu **Otevřít**.
   b) Vyberte **JKS** ze seznamu **Typ databáze klíčů** .
   c) Klepněte na tlačítko **Procházet** a přejděte na adresu *MQ_DATA_PATH*`/web/installations/`*installationName*`/servers/mqweb/resources/security` .
   d) Vyberte úložiště klíčů produktu `key.jks` a klepněte na tlačítko **Otevřít**.
   e) Zadejte heslo, až budete vyzváni. Výchozí heslo je `password`.

f) V nabídce **Soubor databáze klíčů** klepněte na **Změnit heslo**.

g) Zadejte nové heslo pro úložiště klíčů.

6. Povolte ověření klientského certifikátu 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 autentizaci certifikátu klienta. 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 parametru **password** pro `defaultKeyStore` na zakódovanou verzi hesla pro úložiště klíčů produktu `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 **password** pro `defaultKeyStore`.

   d) Změňte hodnotu pro **password** pro `defaultTrustStore` tak, aby odpovídala heslu pro úložiště klíčů produktu `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 **password** pro `defaultTrustStore`.

   e) Odstraňte nebo označte jako komentář následující řádek ze souboru `mqwebuser.xml` :

   ```
   <sslDefault sslRef="mqDefaultSSLConfig"/>
   ```

7. Zadáním příkazu **endmqweb** na příkazový řádek zastavte parametr mqweb.
8. Zadáním příkazu **strmqweb** na příkazový řádek spusťte program mqweb.
9. Použít certifikát klienta k ověření:

   - Chcete-li použít certifikát klienta s produktem IBM MQ Console, nainstalujte certifikát klienta do webového prohlížeče používaného pro přístup k produktu IBM MQ Console. Například, nainstalujte certifikát klienta `user.p12` jako osobní certifikát.
   - Chcete-li použít certifikát klienta s produktem REST API, poskytněte mu certifikát klienta s každým požadavkem REST. Použijete-li metody HTTP POST, PATCH nebo DELETE, musíte poskytnout dodatečné ověření s certifikátem klienta, abyste zabránili útokům typu forgfalz křížového serveru. To znamená, že dodatečné ověření se použije k potvrzení, že pověření, která jsou použita pro ověření požadavku, jsou používána vlastníkem pověření.

     This extra authentication is provided by the `ibm-mq-rest-csrf-token` HTTP header. Nastavte hodnotu záhlaví `ibm-mq-csrf-token` na cokoli včetně prázdného, pak odešlete požadavek.

Příklad

Důležité: V tomto příkladu žádné implementace cURL nepodporují certifikáty podepsané sebou samým, takže musíte použít implementaci cURL , která se bude provádět.

Následující příklad cURL ukazuje, jak vytvořit novou frontu Q1, ve správci front QM1, s ověřením klientského certifikátu. Přesná konfigurace tohoto příkazu cURL závisí na knihovnách, vůči kterým byla vytvořena cURL . Tento příklad je založen na systému Windows s parametrem cURL built against OpenSSL.

- Použijte metodu HTTP POST s prostředkem fronty, ověřením pomocí certifikátu klienta a včetně záhlaví HTTP `ibm-mq-rest-csrf-token` s libovolnou hodnotou. Tato hodnota může být libovolná, včetně prázdné. Parametr `--cert-type` udává, že certifikát je certifikátem PKCS#12 . Parametr `--cert` určuje umístění certifikátu, za nímž následuje dvojtečka,:, a pak heslo certifikátu:

```
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 produktem REST API

Uživatelé produktu REST API se mohou ověřit zadáním svého ID uživatele a hesla v rámci záhlaví HTTP. Chcete-li použít tuto metodu ověření s metodami HTTP, jako jsou např. POST, PATCH a DELETE, musí být také poskytnuto záhlaví HTTP `ibm-mq-rest-csrf-token` , stejně jako ID uživatele a heslo.

Než začnete

- Konfigurujte uživatele, skupiny a role, abyste byli autorizováni používat produkt REST API. Další informace viz téma “Konfigurace uživatelů a rolí” na stránce 498.
- Ujistěte se, že je povoleno základní ověřování HTTP. Zkontrolujte, zda je přítomen následující XML a není označen jako komentář, v souboru `mqwebuser.xml` . Tento kód XML musí být ve značkách produktu `<featureManager>` :

```
<feature>basicAuthenticationMQ-1.0</feature>
```

z/OS V systému z/OSmusíte být uživatel, který má přístup pro zápis k souboru `mqwebuser.xml` pro úpravy tohoto souboru.

Multi Na všech ostatních operačních systémech musíte být privilegovaným uživatelem , abyste mohli upravovat soubor `mqwebuser.xml` .

- Ujistěte se, že používáte zabezpečené připojení, když odešlete požadavky REST. Když je kombinace jména uživatele a hesla zakódována, ale není šifrována, musíte použít zabezpečené připojení (HTTPS), když používáte základní ověření HTTP se serverem REST API.
- Můžete se dotázat na pověření aktuálního uživatele pomocí metody HTTP GET na prostředku `login` , poskytnout informace o základním ověření pro ověření požadavku. Tento požadavek vrátí informace o jménu uživatele a o rolích, které je uživatel přiřazen. Další informace viz GET `/login`.

Postup

1. Zřetězit jméno uživatele pomocí dvojtečky a hesla. Všimněte si, že jméno uživatele rozlišuje velká a malá písmena.

   Například jméno uživatele admin a heslo administrátora se stane následujícím řetězcem:

   ```
   admin:admin
   ```

2. Zakódujte tento řetězec jména uživatele a hesla do kódování base64 .
3. Zahrňte toto zakódované jméno uživatele a heslo do záhlaví HTTP `Authorization: Basic` .

   Například se zakódovaným jménem uživatele admin a heslem admin se vytvoří toto záhlaví:

   ```
   Authorization: Basic YWRtaW46YWRtaW4=
   ```

4. Když použijete metody HTTP POST, PATCH nebo DELETE, musíte poskytnout dodatečné ověření, stejně jako jméno uživatele a heslo.

This extra authentication is provided by the `ibm-mq-rest-csrf-token` HTTP header. Hlavička `ibm-mq-rest-csrf-token` HTTP musí být přítomna v požadavku, ale její hodnota může být libovolná, včetně prázdné.

5. Odešlete svůj požadavek REST do produktu IBM MQ s příslušnými záhlavími.

Příklad

Následující příklad uvádí, jak vytvořit novou frontu Q1, ve správci front QM1, se základním ověřením, v systémech Windows . V příkladu je použita adresa cURL:

- Použijte metodu HTTP POST s prostředkem fronty, ověřováním pomocí základního ověření a včetně záhlaví HTTP `ibm-mq-rest-csrf-token` s libovolnou hodnotou. Tato hodnota může být libovolná, včetně prázdné:

```
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 API služby REST

Uživatelé produktu REST API se mohou ověřit zadáním ID uživatele a hesla do prostředku produktu REST API `login` s metodou 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 dotázat se na protokol v informacích aktuálního uživatele pomocí metody HTTP GET.

Než začnete

- Konfigurujte uživatele, skupiny a role, abyste byli autorizováni používat produkt REST API. Další informace viz téma “Konfigurace uživatelů a rolí” na stránce 498.
- Při výchozím nastavení je název souboru cookie, který obsahuje token LTPA, spuštěn s produktem `LtpaToken2`, a obsahuje příponu, která se může změnit při restartu serveru mqweb. Tento náhodný název souboru cookie umožňuje spuštění více než jednoho parametru mqweb na stejném systému. Pokud však chcete, aby název souboru cookie zůstal konzistentní hodnotou, můžete zadat název, který má soubor cookie použít, pomocí příkazu **setmqweb** . Další informace viz Konfigurace tokenu LTPA.
- Při výchozím nastavení 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.
- Ujistěte se, že používáte zabezpečené připojení, když odešlete požadavky REST. Použijete-li metodu HTTP POST na prostředku `login` , kombinace jména uživatele a hesla, která se odešle s požadavkem, nebude šifrována. Proto musíte použít zabezpečené připojení (HTTPS), když používáte ověření založené na tokenech s produktem REST API. Ve výchozím nastavení nelze použít protokol HTTP s ověřením tokenu LTPA. Můžete povolit, aby token LTPA byl použit nezabezpečenými připojeními HTTP nastavením **secureLTPA** na `False`. Další informace viz Konfigurace tokenu LTPA.
- Můžete se dotázat na pověření aktuálního uživatele pomocí metody HTTP GET na prostředku `login` , čímž poskytnete token LTPA ověření požadavku. Tento požadavek vrátí informace o jménu uživatele a o rolích, které je uživatel přiřazen. Další informace viz GET `/login`.

Postup

1. Přihlášení uživatele:
   a) Použijte metodu HTTP POST na prostředku `login` :

   ```
   https://host:port/ibmmq/rest/v1/login
   ```

   Vložte jméno uživatele a heslo do těla požadavku JSON v následujícím formátu:

```
{
    "username" : name,
    "password" : password
}
```

b) Uložte token LTPA, který je vrácen z požadavku v lokálním úložišti souborů cookie. Ve výchozím nastavení má tento token LTPA předponu `LtpaToken2`.

2. Ověřte požadavky REST s uloženým tokenem LTPA jako soubor cookie s každým požadavkem.

   Pro požadavky, které používají metody HTTP PUT, PATCH nebo DELETE, zahrňte 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 libovolná, včetně prázdné

   b) Zpracujte instrukce, jak odstranit token LTPA z lokálního úložiště souborů cookie.

   Poznámka: Pokud se instrukce nezpracuje 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 o ověření s tokenem 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 založenou na tokenem, v systémech Windows :

- Přihlaste se a přidejte token LTPA s předponou `LtpaToken2`do lokálního úložiště souborů cookie. Informace o jménu uživatele a heslu jsou obsaženy v těle JSON. Parametr `-c` určuje umístění souboru, do kterého se má uložit token:

  ```
  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, ověřováním pomocí tokenu LTPA. Token LTPA s předponou `LtpaToken2` je načten ze souboru `cookiejar.txt` pomocí parametru `-b` . Ochrana CSRF je zajištěna přítomností záhlaví HTTP `ibm-mq-rest-csrf-token` :

  ```
  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 parametru `-b` . Ochrana CSRF je zajištěna přítomností záhlaví HTTP `ibm-mq-rest-csrf-token` . Umístění souboru `cookiejar.txt` je určeno parametrem `-c` tak, aby byl token LTPA 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

V 9.2.0 Vnoření IBM MQ Console do 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 rámce IFrame. Můžete však povolit IFrame pomocí vlastnosti konfigurace produktu **mqConsoleFrameAncestors** na webovém serveru mqweb.

Informace o této úloze

Server mqweb udržuje seznam původu webových stránek, které mohou produkt IBM MQ Console vložit pomocí rámce IFrame. Počátek je kombinací schématu adresy URL, domény a portu, například `https://example.com:1234`.

Konfigurační vlastnost **mqConsoleFrameAncestors** na serveru mqweb můžete použít k určení položek v seznamu.

Ve výchozím nastavení je **mqConsoleFrameAncestors** prázdný, což znamená, že IBM MQ Console nelze vložit do rámce IFrame.

Postup

Zadáním následujícího příkazu určete seznam míst původu webových stránek, který může vložit IBM MQ Console do rámce IFrame:

```
setmqweb properties -k mqConsoleFrameAncestors -v allowedOrigins
```

kde *allowedOrigins* je seznam původu oddělený čárkami. Každý původ by měl sestávat z:

- Název hostitele nebo adresa IP
- Volitelný schéma adresy URL
- Volitelné číslo portu

Všimněte si, že název hostitele může začínat zástupným znakem (*) a číslo portu může také použít zástupný znak (*).

Příklad původu:

```
https://example.com:1234
```

který umožňuje libovolné webové stránce obsluhované z produktu `https://example.com:1234` , aby byla vestavěna IBM MQ Console do rámce IFrame.

```
https://*.example.com:*
```

který povoluje jakoukoli webovou stránku HTTPS s názvem hostitele končícím produktem `example.com`a použitím libovolného portu pro vložení IBM MQ Console do rámce IFrame.

Příklad

Následující příklad umožňuje vložení IBM MQ Console do rámce IFrame z webových stránek obsluhovaných buď z produktu `https://site2.example.com:1234` , nebo z `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

Ve výchozím nastavení webový prohlížeč nepovoluje skripty, jako je skript JavaScript, vyvolat REST API , když skript není ze stejného původu jako REST API. To znamená, že požadavky typu cross-origin nejsou

povoleny. Můžete nakonfigurovat rozhraní CORS (Cross Origin Resource Sharing) tak, aby bylo možné z určených původů povolit požadavky na křížový původ.

Informace o této úloze

K produktu REST API můžete přistupovat prostřednictvím webového prohlížeče, například prostřednictvím skriptu. Protože tyto požadavky jsou z jiného původu do produktu REST API, webový prohlížeč požadavek odmítne, protože se jedná o požadavek s křížovým původem. Původ se liší v případě, že doména, port nebo schéma nejsou stejné.

Máte-li například skript, který je hostován na portálu `http://localhost:1999/` , uvedete požadavek na křížový původ, pokud vydáte HTTP GET na webu hostovaném na serveru `https://localhost:9443/`. Tento požadavek je požadavek na křížový původ, protože čísla portů a schéma (HTTP) se liší.

Požadavky typu cross-origin můžete povolit konfigurací CORS a uvedením původu, které jsou povoleny pro 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
   ```

   Zadání `mqRestCorsAllowedOrigins` určuje povolený původ. Záznam `mqRestCorsMaxAgeInSeconds` určuje dobu (v sekundách), po kterou může webový prohlížeč ukládat výsledky všech kontrol před letem z CORS.
2. Zadáním následujícího příkazu určete původ, který je povolen pro přístup k REST API :

   ```
   setmqweb properties -k mqRestCorsAllowedOrigins -v allowedOrigins
   ```

   kde *allowedOrigins* uvádí původ, ze kterého chcete povolit požadavky mezi původci. Můžete použít hvězdičku obklopenou dvojitými uvozovkami, "*", chcete-li povolit všechny požadavky na křížový původ. Do seznamu odděleného čárkami můžete zadat více než jeden původ, ohraničený dvojitými uvozovkami. Chcete-li povolit žádné požadavky mezi původci, zadejte prázdné uvozovky jako hodnotu pro *allowedOrigins*.
3. Určete dobu v sekundách, po kterou chcete povolit webovému prohlížeči ukládat do mezipaměti výsledky všech předletových kontrol CORS zadáním následujícího příkazu:

   ```
   setmqweb properties -k mqRestCorsMaxAgeInSeconds -v time
   ```

Příklad

Následující příklad ukazuje požadavky typu cross-origin povolené pro produkty `http://localhost:9883`, `https://localhost:1999`a `https://localhost:9663`. Maximální stáří výsledků uložených v mezipaměti pro všechny předletové kontroly CORS 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 s hlavičkou hostitele, která se shoduje s uvedeným seznamem povolených. Je-li použita hodnota záhlaví hostitele, která není na seznamu povolených, je vrácena chyba.

Informace o této úloze

Server mqweb používá virtuální hostitele k definování přípustného seznamu přijatelných záhlaví hostitele. Další informace o virtuálních hostitelích naleznete v dokumentaci 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 pro úpravu souboru `mqwebuser.xml` :

- z/OS V systému z/OSmusíte mít přístup pro zápis k souboru `mqwebuser.xml` .
- Multi U všech ostatních operačních systémů musíte být privilegovaný uživatel.

Postup

1. Otevřete soubor `mqwebuser.xml` . Tento soubor je v jednom z následujících umístění:
   - ALW

     V systému AIX, Linux, and Windows: *MQ_DATA_PATH*`/web/installations/`*installationName*`/servers/mqweb`
   - z/OS

     V systému z/OS: *WLP_user_directory*`/servers/mqweb`

     kde *WLP_user_directory* je adresář, který byl zadán při spuštění skriptu **crtmqweb** za účelem vytvoření definice mqweb serveru.
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>** a vložte kombinaci názvu hostitele a portu, který chcete povolit.

   Tato kombinace může být názvem hostitele a názvem portu, který jste použili v konfiguraci na serveru mqweb. Použijete-li například výchozí konfiguraci produktu `localhost:9443`, můžete chtít použít volbu `localhost:9443` v poli **<hostAlias>** .

   Je-li to nutné, můžete přidat více polí **<hostAlias>** ve značkách **<virtualHost>** , chcete-li povolit 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 provedených v IBM MQ Console a REST API mohou být vytvářeny povolením příkazů správce front a událostí konfigurace a na AIX, Linux, and Windows významných změn stavu se zaznamenává do souborů protokolu mqweb serveru.

Významné změny stavu

ALW

V systému AIX, Linux, and Windowszaznamenává produkt IBM MQ Console významné změny stavu jako zprávy v protokolech na webovém serveru mqweb. Každá zpráva označuje ověřený řídicí název, který požadoval operaci.

Významné změny stavu, například při vytvoření, spuštění, ukončení nebo odstranění správců front jsou protokolovány v souborech `messages.log` a `console.log` webového serveru na úrovni protokolování [AUDIT]. Každá položka protokolu označuje ověřený řídicí název, který požadoval operaci.

Soubory `messages.log` a `console.log` lze nalézt v následujícím umístění:

- ALW V systému AIX, Linux, and Windows:
  MQ_DATA_PATH\web\installations*installationName*\servers\mqweb\logs

Další informace o konfiguraci úrovní protokolování mqweb serverů najdete v tématu Konfigurace protokolování.

Události příkazů a konfigurace

Volitelně můžete povolit příkazy a události konfigurace ve správci front, a poskytnout tak informace o většině aktivit IBM MQ Console a REST API . Například vytváření kanálů a zjišťování front příkazů generování příkazů a konfiguračních událostí. Další informace o povolení událostí příkazů a konfiguračních událostí naleznete v tématu Řízení konfigurace, příkazů a událostí modulu protokolování.

Pro zprávy těchto příkazů a konfiguračních událostí je pole MQIACF_EVENT_ORIGIN nastaveno na hodnotu MQEVO_REST a pole MQCACF_EVENT_APPL_IDENTITY nahlásí prvních 32 znaků ověřeného názvu činitele. Má-li uživatel roli **MQWebAdmin** nebo **MQWebAdminRO** , pole MQCACF_EVENT_USER_ID hlásí ID uživatele mqweb serveru, nikoli jméno uživatele činitele, který příkaz vydal. Má-li však uživatel roli **MQWebUser** , MQCACF_EVENT_USER_ID ohlásí jméno uživatele činitele, který příkaz vydal.

Související pojmy

“Auditování” na stránce 466
Můžete zkontrolovat narušení zabezpečení nebo pokusy o narušení pomocí zpráv událostí. Zabezpečení vašeho systému můžete také zkontrolovat pomocí IBM MQ Explorer.

Aspekty zabezpečení pro produkty IBM MQ Console a REST API v systému z/OS

Příkazy IBM MQ Console a REST API mají funkce zabezpečení, které řídí, zda uživatel může vydávat, zobrazovat nebo měnit příkazy. Příkazy se poté předají správci front a poté je zabezpečení správce front používáno k řízení, zda má uživatel povoleno zadávat příkaz tomuto konkrétnímu správci front.

Postup

1. Ujistěte se, že ID uživatele spuštěné úlohy mqweb serveru má příslušná oprávnění k vydání určitých příkazů PCF a k přístupu k určitým frontám. Další informace viz téma “Oprávnění požadované uživatelským ID úlohy spuštěné serverem mqweb” na stránce 522.
2. Ujistěte se, že všichni uživatelé, kterým je udělena role `MQWebUser` , mají příslušné 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, které má uděleno ID uživatele k provedení na správci front, a musí jim být udělen přístup ke stejným systémovým frontám jako adresní prostor mqweb server.

   ID uživatele úlohy spuštěné úlohou mqweb serveru musí být uděleno alternativnímu uživateli přístup ke všem uživatelům přiřazeným k roli `MQWebUser` .

   Další informace o udělení příslušných oprávnění pro uživatele s rolí `MQWebUser` viz “Přístup k prostředkům produktu IBM MQ vyžadovaným pro použití produktu MQ Console nebo REST API” na stránce 523.
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 524.

z/OS Oprávnění požadované uživatelským ID úlohy spuštěné serverem mqweb

V systému z/OSvyžaduje ID uživatele úlohy mqweb serveru určité oprávnění k vydávání příkazů PCF a k přístupu k systémovým prostředkům.

ID uživatele spuštěné úlohy serveru mqweb vyžaduje:

- Identifikátor uživatele (UID) produktu z/OS , který má být schopen používat produkt 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 produktu z/OS UNIX System Services.
- Přístup pro čtení a zápis do adresáře uživatelů produktu Liberty vytvořeného pomocí skriptu **crtmqweb** .
- Oprávnění pro připojení ke správci front. Udělte uživateli úlohy mqweb ID uživatele spuštěné úlohy *READ* pro přístup k profilu produktu `hlq.BATCH` ve třídě MQCONN.
- Oprávnění k vydávání příkazů IBM MQ a přístup k určitým frontám. Tyto podrobnosti jsou popsány v publikaci “IBM MQ Console -požadované profily zabezpečení příkazu” na stránce 224, “Zabezpečení systémové fronty” na stránce 200a “Profily pro zabezpečení kontextu” na stránce 211.
- Oprávnění k přihlášení k odběru tématu SYSTEM.FTE , aby bylo možné použít produkt REST API for MFT. Udělte uživateli mqweb ID uživatele spuštěné úlohy *ALTER* pro přístup k profilu produktu `hlq.SUBSCRIBE.SYSTEM.FTE` ve třídě MXTOPIC.
- Pokud konfigurujete registr SAF, přistupte k různým profilům zabezpečení. Další informace viz “Konfigurace registru SAF pro IBM MQ Console a REST API” na stránce 505.

Ověření připojení

If your queue manager has been configured to require that all batch applications provide a valid user ID and password, by setting CHKLOCL(REQUIRED), you must give the mqweb server started task user ID *AKTUALIZOVAT* access to the `hlq.BATCH` profile in the MQCONN class.

Tento orgán způsobí, že ověření připojení bude fungovat v režimu CHKLOCL (OPTIONAL) pro ID uživatele spuštěné úlohy mqweb serveru.

Pokud jste správce front nekonfigurovali tak, aby vyžadoval, aby všechny dávkové aplikace poskytovaly platné ID uživatele a heslo, stačí zadat ID uživatele, které spouští úlohu *READ* úlohy serveru mqweb v rámci třídy MQCONN pro přístup k profilu produktu `hlq.BATCH` .

Další informace o CHCKLOCL viz “Použití produktu CHCKLOCL v lokálně vázaných aplikacích” na stránce 191.

Přístup k prostředkům produktu IBM MQ vyžadovaným pro použití produktu MQ Console nebo REST API

Operace prováděné v produktu MQ Consolenebo REST APIuživatelem v roli `MQWebUser` se provádí pod kontextem zabezpečení daného uživatele.

Informace o této úloze

Další informace o rolích v produktu MQ Console a REST APInaleznete v příručce “Role na IBM MQ Console a REST API” na stránce 507 .

Pomocí následujícího postupu udělte uživateli v roli produktu `MQWebUser` přístup k prostředkům správce front vyžadovaným pro použití produktu MQ Console nebo produktu REST API.

Postup

1. Udělte uživateli produktu `mqweb server started task` alternativní uživatelský přístup ke každému ID uživatele v roli `MQWebUser` .

   Tuto akci provádějte v každém správci front, který uživatelé budou spravovat prostřednictvím produktu MQ Console nebo REST API.

   Následující ukázkové příkazy produktu RACF můžete použít k udělení uživatelského jména ID uživatele produktu `mqweb server started task` pro uživatele 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
Jedná se o předponu profilu, která může být buď název správce front, nebo název skupiny sdílení front

userId
Je uživatel v roli `MQWebUser`

mqwebUserId
Je ID uživatele produktu `mqweb server started task`

Poznámka: Používáte-li zabezpečení se smíšenými případy, použijte raději třídu MXADMIN než třídu MQADMIN.

2. Udělte každému uživateli v roli `MQWebUser` přístup k systémovým frontám, které jsou nezbytné pro použití produktů MQ Console a REST API.

   Chcete-li to provést, pro SYSTEM.ADMIN.COMMAND.QUEUE a SYSTEM.REST.REPLY.QUEUE, udělte každému uživateli příkaz UPDATE k třídám MQQUEUE nebo MXQUEUE v závislosti na tom, zda se používá zabezpečení se smíšeným případem.

   Tuto akci je třeba provést ve všech správcích front, které uživatel bude spravovat prostřednictvím produktu REST API, včetně vzdálených správců front spravovaných prostřednictvím brány administrative REST API.
3. Chcete-li uživateli v roli produktu `MQWebUser` povolit administraci vzdálených správců front, udělte uživateli příkaz UPDATE přístup k profilu ve třídě MQQUEUE nebo MXQUEUE chránící přenosovou frontu používanou k odesílání příkazů vzdálenému správci front. Všimněte si, že je třeba udělit uživateli příkaz UPDATE přístup ke správci front brány.

   V případě vzdáleného správce front udělte přístup pro stejného uživatele k vložení do přenosové fronty použité k odeslání zpráv s odpovědí na příkazy zpět do správce front brány.
4. Udělte uživatelům v roli `MQWebUser` přístup ke všem dalším prostředkům vyžadovaným k provádění operací podporovaných produktem MQ Console a produktem REST API.

   Přístup potřebný k:

   - Provedení operací v REST APIje popsáno v sekcích *Požadavky na zabezpečení* jednotlivých prostředků REST API .
   - Příkazy výdejky podle MQ Console jsou popsány v části “IBM MQ Console -požadované profily zabezpečení příkazu” na stránce 224

z/OS Konfigurace TLS pro REST API a IBM MQ Console na z/OS

V systému z/OSmůžete nakonfigurovat parametr mqweb server tak, aby používal svazek klíčů RACF k ukládání certifikátů pro zabezpečená připojení pomocí TLS a ověření klientských certifikátů.

Než začnete

Chcete-li dokončit tento postup, musíte být uživatel, který má přístup pro zápis k souboru `mqwebuser.xml` a oprávnění k práci s klíči SAF.

Informace o této úloze

Výchozí konfigurace parametru mqweb server používá úložiště klíčů produktu Java pro server a důvěryhodné certifikáty. V systému z/OSmůžete nakonfigurovat parametr mqweb server tak, aby používal svazek klíčů RACF místo úložišť klíčů Java . Server lze také nakonfigurovat tak, aby umožnil uživatelům ověření pomocí certifikátu klienta.

Informace o používání klíčových řetězců RACF v produktu Libertynajdete v tématu Liberty: Keystores .

Postupujte podle této procedury a nakonfigurujte server mqweb tak, aby používal svazek klíčů produktu RACF , a volitelně konfigurujte ověření klientských certifikátů. Tento postup popisuje kroky nezbytné k vytvoření a použití certifikátů podepsaných s vašimi certifikáty certifikačních autorit (CA). Pro produkci můžete raději použít certifikáty získané od externí certifikační autority.

Postup

1. Vytvořte certifikát certifikační autority (CA), který se použije 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 s 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 pro mqweb server.

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 mqweb serveru 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. FTP exportovaný certifikát CA v binárním souboru na pracovní stanici a importujte jej do vašeho prohlížeče jako certifikát certifikačního orgánu.
6. Volitelné: Chcete-li konfigurovat ověření klientského certifikátu, vytvořte a exportujte certifikát klienta.
   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 mqweb serveru 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:

- Používáte-li základní registr, pole Obecné jméno v certifikátu se porovnává s uživatelem v registru.
- Pokud používáte registr SAF a tento certifikát se nachází v databázi RACF , použije se vlastník certifikátu zadaný parametrem **ID** při vytváření certifikátu.
- Používáte-li 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) FTP exportovaný certifikát v binární podobě do vaší pracovní stanice. Chcete-li použít certifikát klienta s produktem IBM MQ Console, importujte 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 zadán při spuštění skriptu **crtmqweb** za účelem vytvoření definice mqweb serveru.

   Proveďte následující změny, abyste nakonfigurovali parametr mqweb server pro použití svazku klíčů RACF :

   a) Odebrat nebo označit komentář jako 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 mqweb serveru.
   - *keyring* je název svazku klíčů RACF .
   - *mqwebServerCert* je jmenovka certifikátu mqweb serveru.

   Notes: Hodnota parametru **keyStore password** se ignoruje.

8. Restartujte server mqweb tím, že zastavíte a znovu spustíte spuštěnou úlohu mqweb server.
9. Volitelné: Použít certifikát klienta k ověření:

   - Chcete-li použít certifikát klienta s produktem IBM MQ Console, zadejte adresu URL pro produkt MQ Console ve webovém prohlížeči, do kterého jste instalovali certifikát klienta.
   - Chcete-li použít certifikát klienta s rozhraním API služby REST, poskytněte certifikát klienta s každým požadavkem REST.

   Notes:

   a. Pokud používáte pouze certifikáty pro ověření vůči serveru IBM MQ Console, může prohlížeč zobrazit seznam certifikátů, ze kterých si můžete vybírat.

   b. Chcete-li použít jiný certifikát, může být nutné zavřít a restartovat prohlížeč.

c. Pokud používáte certifikáty klienta, které nejsou v databázi RACF , můžete použít filtrování názvů certifikátů produktu RACF k mapování atributů certifikátu na ID uživatele. Příklad:

```
RACDCERT ID(DEPT3USR) MAP SDNFILTER(OU=DEPT1.C=US)
```

mapuje certifikáty s rozlišujícím názvem subjektu obsahujícím OU=DEPT1 a C=US k ID uživatele DEPT3USR.

Výsledky

Pro produkt IBM MQ Console a REST APIjste nastavili rozhraní TLS.

ALW Správa klíčů a certifikátů v systému AIX, Linux, and Windows

V systému AIX, Linux, and Windowsmůžete použít příkazy **runmqckm** a **runmqakm** ke správě klíčů, certifikátů a žádostí o certifikáty.

Příkaz **runmqckm** poskytuje funkce, které jsou podobné funkcím **iKeyman**, a **runmqakm** , poskytuje funkce podobné funkcím **gskitcapicmd**. Před použitím **runmqckm** nebo **runmqakm**se ujistěte, že jsou proměnné prostředí systému správně konfigurovány spuštěním příkazu **setmqenv** .

Příkaz **runmqckm** vyžaduje, aby byla nainstalována komponenta prostředí JRE produktu IBM MQ . Pokud tato komponenta není instalována, můžete místo toho použít příkaz **runmqakm** .

Potřebujete-li spravovat certifikáty TLS způsobem, který vyhovuje standardu FIPS, použijte namísto příkazu **runmqckm** příkaz **runmqakm** . Je tomu tak proto, že příkaz **runmqakm** podporuje silnější šifrování.

Použijte příkazy **runmqckm** a **runmqakm** k provedení následujících úloh:

- Vytvořte typ souborů databáze klíčů CMS, které produkt IBM MQ vyžaduje
- Vytvořit žádosti o certifikát
- Importovat osobní certifikáty
- Importovat certifikáty CA
- Spravovat certifikáty podepsané sebou samým

Související informace

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 541 .

ALW Příkazy pro databázi klíčů CMS pouze na systému AIX, Linux, and Windows

Pomocí příkazů **runmqckm** a **runmqakm** můžete spravovat klíče a certifikáty pro databázi klíčů CMS.

-keydb -changepw
Změňte heslo pro databázi klíčů CMS:

Pomocí příkazu **runmqckm** :

```
-keydb -changepw -db filename -pw password -new_pw new_password
-stash
```

Pomocí příkazu **runmqakm** :

```
-keydb -changepw -db filename -pw password -new_pw new_password
-stash -fips -strong
```

-keydb -vytvořit
Vytvořte databázi klíčů CMS:

Pomocí příkazu **runmqckm** :

```
-keydb -create -db filename -pw password -type cms -expire days
-stash
```

Pomocí příkazu **runmqakm** :

```
-keydb -create -db filename -pw password -type cms -expire days
-stash -fips -strong
```

-keydb -stashpw
Uložte heslo databáze klíčů CMS do souboru:

Pomocí příkazu **runmqckm** :

```
-keydb -stashpw -db filename -pw password
```

Pomocí příkazu **runmqakm** :

```
-keydb -stashpw -db filename -pw password -fips
```

-cert -getdefault

Poznámka: Výchozí certifikát není produktem IBM MQ 8.0podporován. Měli byste použít konfiguraci popisku certifikátu, jak je popsáno v tématu “Digitální certifikáty certifikátu, základní informace o požadavcích” na stránce 24.

Získejte výchozí osobní certifikát:

Pomocí příkazu **runmqckm** :

```
-cert -getdefault -db filename -pw password
```

Pomocí příkazu **runmqakm** :

```
-cert -getdefault -db filename -pw password -fips
```

-cert-upravit
Upravit certifikát.

Poznámka: V současné době je jediným polem, které lze upravit, pole důvěryhodnosti certifikátu.

Pomocí příkazu **runmqckm** :

```
-cert -modify -db filename -pw password -label label
-trust enable|disable
```

Pomocí příkazu **runmqakm** :

```
-cert -modify -db filename -pw password -label label
-trust enable|disable -fips
```

-cert -setdefault

Poznámka: Výchozí certifikát není podporován produktem IBM MQ 8.0 nebo novějším. Měli byste použít konfiguraci popisku certifikátu, jak je popsáno v tématu “Digitální certifikáty certifikátu, základní informace o požadavcích” na stránce 24.

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 .

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** :

```
-keydb -create -db filename -pw password -type cms
| pkcs12
```

Pomocí příkazu **runmqakm** :

```
-keydb -create -db filename -pw password -type cms
-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 .

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, uvědomte si, že **runmqckm** a **strmqikm** 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, neboť 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, uvědomte si, že **runmqckm** a **strmqikm** 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, neboť 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, uvědomte si, že **runmqckm** a **strmqikm** 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, neboť 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, uvědomte si, že **runmqckm** a **strmqikm** 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, neboť 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, uvědomte si, že **runmqckm** a **strmqikm** 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, neboť 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, uvědomte si, že **runmqckm** a **strmqikm** 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, neboť 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, uvědomte si, že **runmqckm** a **strmqikm** 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, neboť 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, uvědomte si, že **runmqckm** a **strmqikm** 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, neboť 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, uvědomte si, že **runmqckm** a **strmqikm** 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, neboť 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, uvědomte si, že **runmqckm** a **strmqikm** 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, neboť 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, uvědomte si, že **runmqckm** a **strmqikm** 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, neboť 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, uvědomte si, že **runmqckm** a **strmqikm** 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, neboť 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, uvědomte si, že **runmqckm** a **strmqikm** 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, neboť 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, uvědomte si, že **runmqckm** a **strmqikm** 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, neboť 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, uvědomte si, že **runmqckm** a **strmqikm** 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, neboť 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, uvědomte si, že **runmqckm** a **strmqikm** 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, neboť 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, uvědomte si, že **runmqckm** a **strmqikm** 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, neboť 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, uvědomte si, že **runmqckm** a **strmqikm** 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, neboť 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 .

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 94. 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`.
-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 ICC používá algoritmy ověřené dle 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`.

*Tabulka 94. Volby, které lze použít s volbami **runmqckm** a **runmqakm** (pokračování)*	
Parametr	**Popis**
-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 certifikáty certifikátu, základní informace o požadavcích" na stránce 24.
-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 certifikáty certifikátu, základní informace o požadavcích" na stránce 24.
-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 .
-showOID	Zobrazí úplný certifikát nebo žádost o certifikát.
-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.

*Tabulka 94. Volby, které lze použít s volbami **runmqckm** a **runmqakm** (pokračování)*	
Parametr	**Popis**
-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.
-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.
-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.

*Tabulka 94. Volby, které lze použít s volbami **runmqckm** a **runmqakm** (pokračování)*	
Parametr	**Popis**

-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	Došlo k chybě kódování/dekódování ASN.1 .
3	Při inicializaci kodéru/dekodéru ASN.1 došlo k chybě.
4	Došlo k chybě kódování/dekódování ASN.1 kvůli indexu mimo rozsah nebo neexistujícímu volitelnému poli.
5	Došlo k chybě databáze.
6	Při otevírání databázového souboru došlo k chybě. 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 se nepodařilo 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.

Kód chyby	Chybová zpráva
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.
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.

Kód chyby	Chybová zpráva
47	Doba platnosti nezahrnuje dnešek 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.
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.

Kód chyby	Chybová zpráva
75	Při načítání CMS došlo k chybě.
76	Došlo k chybě související s šifrovacím hardwarem.
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.
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	Při dekódování dat Base64-encoded došlo k chybě.
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.

Kód chyby	Chybová zpráva
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 .
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 na soubor 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, které jste zadali, přesahuje povolené období platnosti.
130	Heslo je příliš krátké; musí obsahovat alespoň {0} znaků.
131	Heslo musí obsahovat alespoň jednu číselnou číslici.

Kód chyby	Chybová zpráva
132	Všechny znaky v hesle jsou buď abecední, nebo číselné.
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)
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	Došlo k selhání funkce šifrovacího objektu.
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.

Kód chyby	Chybová zpráva
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.
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 MD5 a 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.

Kód chyby	Chybová zpráva
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.

V 9.2.0 V 9.2.0 Ochrana hesel v konfiguračních souborech komponenty IBM MQ

Chcete-li používat určité funkce produktu IBM MQ, je možné, že hesla budou muset být dodána buď přímo do produktu IBM MQ , nebo uvnitř konfiguračních souborů, které tato funkce čte. Z produktu IBM MQ 9.2.0je implementován nový systém ochrany hesla, který umožňuje ochranu hesel v těchto konfiguračních souborech.

Měli byste chránit hesla v konfiguračních souborech. Následující seznam vysvětluje obecnou terminologii používanou pro jednotlivé komponenty:

Počáteční klíč
Šifrovací klíč, který poskytnete pro použití v procesu šifrování.

Pro každou z uvedených komponent můžete dodat počáteční soubor s klíči, který obsahuje šifrovací klíč, který se má použít při ochraně nebo čtení hesel uložených v konfiguračním souboru dané komponenty.

Soubor musí obsahovat jeden řádek s alespoň jedním znakem.

Délka šifrovacího klíče není omezena ani požadována, avšak váš soubor s klíči by měl obsahovat alespoň 16 znaků. Váš soubor může například obsahovat následující položky:

```
Th1sIs@n3Ncypt|onK$y
```

Kromě toho by měl vámi zadaný počáteční soubor s klíči:

- Obsahuje jedinečný šifrovací klíč.
- Být dostatečně chráněni pomocí oprávnění operačního systému.

Výchozí počáteční klíč
Výchozí použitý šifrovací klíč, pokud při šifrování dat nezadáte počáteční klíč. Neměli byste však **používat** výchozí počáteční klíč.

Řetězec prostého textu
Řetězec, který je zašifrovaný, obvykle heslo

Zakódované heslo
Řetězec, který obsahuje šifrované heslo ve formátu, kterému rozumí IBM MQ.

Důležité: Zakódované 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 553

- “IBM MQ Internet Pass-Thru” na stránce 553
- Deprecated “IBM MQ Bridge to blockchain” na stránce 554
- Deprecated “IBM MQ Bridge to Salesforce” na stránce 555
- V 9.2.3 “Klienti IBM MQ používající kryptografický hardware” na stránce 555

Advanced Message Security

Klienti Advanced Message Security (AMS) Java vyžadují přístup k úložišti klíčů, které obsahuje soukromé klíče, aby ochránili zprávu.

V 9.2.2 Advanced Message Security (AMS) Klienti MQI nebo správci front konfigurovaní 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 přistoupit k tyto, heslo musí být poskytnuto v konfiguračním souboru AMS nazvaném `keystore.conf`. Použijte příkaz **runamscred** k ochraně citlivých informací obsažených v souboru `keystore.conf` . Příklad:

```
runamscred -f <keystore configuration file>
```

Příkaz **runamscred** chrání citlivé parametry v uvedeném souboru pomocí příznaku **-f** .

V 9.2.2 Do instalace produktu IBM MQ byly přidány 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:

1. V 9.2.2 Chcete-li zajistit kompatibilitu, použijte program Java **runamscred** k ochraně konfiguračních souborů, které mají být použity s klienty Java AMS , a program MQI **runamscred** k ochraně konfiguračních souborů, které mají být použity s klienty MQI AMS .
2. Měli byste ověřit, zda byly po spuštění příkazu **runamscred**chráněny všechny nezbytné citlivé informace.
3. Chráněný soubor můžete dodat jako normální pro aplikace s povoleným produktem AMS .

Chcete-li přepsat nebo poskytnout počáteční soubor s klíči, který se má použít během běhového prostředí aplikací AMS , nebo při ochraně konfiguračního souboru úložiště klíčů pomocí produktu **runamscred**, použijte jeden z následujících čtyř mechanizmů. V pořadí podle priority se jedná o:

1. Parametr **-sf** (pouze**runamscred**)
2. proměnná prostředí MQS_AMSCRED_KEYFILE
3. Parametr **amscred.keyfile** v konfiguračním souboru
4. Výchozí počáteční soubor s klíči, pokud není uvedena žádná z výše uvedených voleb.

Upozornění: V 9.2.2 Neměli byste používat výchozí počáteční klíč.

Před IBM MQ 9.2 byl 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 agentovi, koordinaci a příkazové správce front 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 “Šifrování uložených pověření v produktu MFT” na stránce 557.

Chcete-li chránit citlivé informace uložené v těchto souborech, použijte příkaz fteObfuscate v uvedeném souboru s použitím příznaku **-f** . Příklad:

```
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. Měli byste ověřit, zda byly po spuštění příkazu **fteObfuscate**chráněny všechny nezbytné citlivé informace.
2. Chráněný soubor můžete dodat jako normální MFT.

Za běhu poskytněte počáteční soubor s klíči pro použití prostřednictvím následujících tří mechanizmů. V pořadí podle priority se jedná o:

1. Pomocí systémové vlastnosti Java .
   - V 9.2.0.15 Před IBM MQ 9.2.0 Fix Pack 15byl název této systémové vlastnosti Java chybně zapsán v kódu produktu jako `com.ibm.wqmfte.cred.keyfile`. V produktu IBM MQ 9.2.0 Fix Pack 15je pravopis názvu vlastnosti opraven na hodnotu `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 9.2.0 Fix Pack 15použijte vlastnost `com.ibm.wqmfte.cred.keyfile`.
2. V souborech vlastností agenta, modulu protokolování, příkazu 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 příznak **-sp** *0* .

IBM MQ Internet Pass-Thru

Konfigurační soubor IBM MQ Internet Pass-Thru (MQIPT) může obsahovat hesla pro přístup k různým prostředkům a také heslo pro administraci produktu MQIPT .

Tato hesla můžete chránit pomocí příkazu **mqiptPW** dodaného 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 se má použít, prostřednictvím následujících čtyř mechanizmů. V pořadí podle priority se jedná o:

1. Prostřednictvím parametru **-sf** při spouštění 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 pomocí nového systému; to znamená, že konfigurační soubory nejsou kompatibilní se staršími verzemi produktu MQIPT.

Chcete-li chránit hesla úložiště klíčů pomocí starého systému 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** . Chcete-li například vygenerovat konfiguraci se specifickým počátečním souborem s klíči, postupujte takto:

```
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; to 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 verzích od 22. listopadu 2022 (viz Oznamovací dopis USA 222-341).

- V 9.2.0.21 Removed Pro Long Term Supportse IBM MQ Bridge to blockchain odebere v IBM MQ 9.2.0 CSU 21.

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; to 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).

Klienti IBM MQ používající kryptografický hardware

V 9.2.3

Klienty IBM MQ můžete nakonfigurovat tak, aby používaly šifrovací hardware PKCS #11 k ukládání soukromých klíčů a certifikátů používaných v komunikacích TLS. Chcete-li přistupovat k zařízením PKCS #11 , musíte zadat heslo jako součást konfiguračního řetězce dodaného do produktu IBM MQ client.

Důležité: Hesla dodaná prostřednictvím MQSCO.Řetězec struktury **SSLCryptoHardware** nebo atribut správce front **SSLCRYP** nelze tímto mechanizmem chránit.

Toto heslo můžete chránit pomocí příkazu **runp11cred** , který se nachází ve složce bin v kořenovém adresáři instalace produktu IBM MQ .

Příkaz **runp11cred** vás vyzve k bezpečnému zadání hesla pro ochranu a vrátí řetězec, který je třeba zkopírovat do konfiguračního řetězce šifrovacího hardwaru.

Pokud je například GSK_PKCS11 :

```
GSK_PKCS11=/usr/lib/pkcs11/
PKCS11_API.so;tokenlabel;Passw0rd;SYMMETRIC_CIPHER_ON
```

pak po zobrazení výzvy zadejte **Passw0rd**. **runp11cred** vrací řetězec, který vypadá podobně jako následující:

```
<P11>!2!0TyDxrRaS6JUsjON9zfK6S4wEHmSNF0/ZsOdCaTD2dc=!MdpCoxGnFqPtZ1dTLQ58kg==
```

Zkopírujte řetězec tučně namísto řetězce **Passw0rd** v řetězci GSK_PKCS11 :

```
GSK_PKCS11=/usr/lib/pkcs11/PKCS11_API.so;tokenlabel;<P11>!2!
0TyDxrRaS6JUsjON9zfK6S4wEHm SNF0/ZsOdCaTD2dc=!
MdpCoxGnFqPtZ1dTLQ58kg==;SYMMETRIC_CIPHER_ON
```

Chcete-li chránit heslo pomocí specifického počátečního klíče, použijte jeden z následujících mechanismů. V pořadí podle priority se jedná o:

1. Parametr **-sf** (pouze příkaz**runp11cred**)
2. proměnná prostředí MQS_SSLCRYP_KEYFILE
3. **SSLCryptoHardwareKeyFile** Atribut SSL Stanza (pouzeIBM MQ client)
4. Výchozí počáteční soubor s klíči, pokud není uvedena žádná z výše uvedených voleb.

Upozornění: Neměli byste používat výchozí počáteční klíč.

Ochrana podrobností ověření databáze

Pokud používáte ověření jména uživatele a hesla pro připojení ke správci databází, můžete je uložit do úložiště pověření XA produktu MQ , abyste se vyhnuli ukládání hesla do prostého textu v souboru `qm.ini` .

Aktualizujte XAOpenString pro správce prostředků

Chcete-li použít úložiště pověření, musíte upravit XAOpenString v souboru `qm.ini` . Řetězec se používá pro připojení ke správci databází. Do pole XAOpenString můžete určit, kde se má nahradit jméno uživatele a heslo, určete výměnná pole.

- Pole +USER+ se nahradí hodnotou jména uživatele uloženou v úložišti XACredentials.
- Pole +PASSWORD+ je nahrazeno hodnotou hesla uloženou v úložišti XACredentials.

Následující příklady ukazují, jak upravit XAOpenString tak, aby používal soubor pověření pro připojení k databázi.

Připojování 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 pověřením pro databázi do úložiště pověření XA produktu MQ

Poté, co aktualizujete soubor `qm.ini` s nahraditelnými řetězci pověření, musíte přidat jméno uživatele a heslo do úložiště pověření MQ pomocí příkazu **setmqxacred** . **setmqxacred** můžete také použít k úpravě existujících pověření, odstranění pověření nebo seznamu 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, znovu zadejte příkaz **setmqxacred** s novým uživatelským jménem a heslem:

```
setmqxacred -m QM1 -x mydb2 -u user3 -p Password4
```

Aby se změny projevily, je třeba restartovat správce front.

Odstranění pověření

Následující příkaz odstraní pověření:

```
setmqxacred -m QM1 -x mydb2 -d
```

Výpis pověření

Následující příkaz vypíše seznam 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 testovací účely nebo pro účely vyhodnocení v chráněném prostředí. Avšak v produkčním prostředí musíte vhodně kontrolovat, 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 produkt MFT

Správa oprávnění pro prostředky specifické pro produkt MFT

“Použití Advanced Message Security s Managed File Transfer” na stránce 621

Tento scénář vysvětluje, jak nakonfigurovat produkt Advanced Message Security , aby poskytoval důvěrnost dat 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 stavu agentů MFT

V 9.2.0 V 9.2.0 Šifrování uložených pověření v produktu MFT

Managed File Transfer (MFT) vyžaduje několik ID uživatelů a pověření, která jsou uložena ve dvou souborech XML a vy můžete zamlžit tyto příkazy pomocí příkazu **fteObfuscate** . V produktu 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 správcům front příkazů. Pověření pro přístup k úložištím klíčů pro zabezpečená připojení ke správcům front jsou rovněž uložena ve stejném souboru.

Podrobné informace o hodnotách vlastností, které definují umístění souboru `MQMFTCredentials.xml` , naleznete v příručce “Ověřování připojení MFT a IBM MQ” na stránce 560 .

ProtocolBridgeCredentials.xml

Tento soubor obsahuje ID uživatele a pověření pro připojení k serverům protokolu.

Šifrování pověření pomocí příkazu `fteObfuscate`

V příkazu IBM MQ 9.2.0přijímá příkaz **`fteObfuscate`** následující parametry:

- **`credentialsFileName`**, což je povinné
- **`protection mode`**, **`credentialsKeyFile`**a **`outputFileName`**, všechny z nich jsou volitelné

Podrobnosti o parametrech viz **`fteObfuscate`** .

Pokud neuvedete režim ochrany nebo soubor klíčů 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 klíčů pověření, příkaz pracuje jako v předchozích vydáních produktu. Obdržíte varovnou zprávu na konzole označující použití zamítnuté ochrany.

Uvedete-li režim ochrany `0`a uvedete soubor s klíči pověření, obdržíte při použití režimu ochrany `0`chybový výstup na konzole označující, že není platný pro zadání souboru klíčů.

Pokud uvedete režim ochrany `1`a neuvedete soubor klíčů pověření, příkaz použije nejnovější algoritmus, ale s pevným klíčem pro zašifrování pověření.

Pokud uvedete režim ochrany `1`a uvedete soubor s klíči pověření, příkaz zašifruje pověření s použitím nejnovějšího algoritmu.

Pokud uvedete režim ochrany `1`nebo neuvedete režim ochrany a uvedete soubor klíčů pověření, který neexistuje, je chyba na výstupu na konzole označující, že soubor neexistuje.

Pokud uvedete režim ochrany `1`nebo neuvedete režim ochrany a uvedete soubor klíčů pověření, který není čitelný, výstup na konzole indikuje, že soubor nelze číst.

V 9.2.4 Pokud uvedete režim ochrany `2`a neuvedete soubor s klíči pověření, příkaz použije režim ochrany `2` k zašifrování pověření pomocí nejnovějšího algoritmu a pevný klíč k zašifrování.

V 9.2.4 Pokud uvedete režim ochrany `2`a uvedete soubor s klíči pověření, příkaz použije režim ochrany `2` k zašifrování pověření pomocí nejnovějšího algoritmu a uživatele, který je uvedený klíč k šifrování.

V 9.2.4 Pokud uvedete režim ochrany `2`nebo neuvedete režim ochrany a uvedete soubor klíčů pověření, který neexistuje, je chyba na výstupu na konzole označující, že soubor neexistuje.

V 9.2.4 Pokud uvedete režim ochrany `2`nebo neuvedete režim ochrany a uvedete soubor klíčů pověření, který není čitelný, výstup na konzole indikuje, že soubor nelze číst.

Dešifrování pověření

Cestu k počátečnímu souboru klíčů můžete zadat na různých místech. Chcete-li dešifrovat pověření, která byla šifrována pomocí výchozího jiného klíče, než je výchozí klíč, název souboru obsahujícího počáteční klíč musí být poskytnut produktu MFT jedním z následujících způsobů, v tomto pořadí přednosti:

1. Příklad použití vlastnosti Java Virtual Machine (JVM) `com.ibm.wqmfte.cred.keyfile`, například:

   ```
   -Dcom.ibm.wmqfte.cred.keyfile=/usr/hime/credkeyfile.key
   ```

2. Nastavením vlastnosti v souboru vlastností agenta, příkazu, koordinace nebo zapisovače protokolu. Název souboru vlastností a vlastnost, kterou je třeba v ní nastavit, jsou zobrazeny 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 přidání vlastností do jednotlivých souborů vlastností můžete přidat vlastnost **commonCredentialsKeyFile** do existujícího obecného souboru `installation.properties` , takže agent, modul protokolování a příkazy budou moci používat stejnou vlastnost.

Možná jste definovali různé vlastnosti produktu **CredentialsKeyFile** ve více umístěních, takže cesta k souboru s klíči pověření, která se používá pro:

- Agent a modul protokolování se protokoluje do souboru `output0.log` pro daného agenta nebo modul protokolování.
- Příkazy se zobrazí na konzole.

Systémová vlastnost Java **com.ibm.wqmfte.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 se počáteční soubor klíčů stále nenajde a nastavíte režim ochrany na příkazu **fteObfuscate** na 1, agent zaprotokoluje chybovou zprávu do souboru `output0.log` .

Pokud jste v příkazu **fteObfuscate** nastavili režim ochrany na `0` , do protokolu se zaprotokoluje varovná zpráva, která označuje zamítnutí.

Modul protokolování a příkazy postupují podle stejných kroků při hledání počátečního souboru s klíči.

Most protokolů a most Connect:Direct

Protokol mostu protokolu používá soubor vlastností, `ProtocolBridgeProperties.xml`pro připojení k serverům FTP, SFTP a FTPS. Tento soubor vlastností obsahuje atributy připojení potřebné pro připojení k těmto serverům.

Restart agenta mostu je požadován, pokud upravíte hodnotu atributů **credentialsFile** nebo **credentialsKeyFile** v souboru `ProtocolBridgeProperties.xml` .

Jeden z atributů je **credentialsFile**a hodnota obsahuje cestu k souboru XML obsahující UID, nebo PWD, nebo klíč potřebný pro připojení k těmto serverům. Výchozí hodnota atributu je *ProtocolBridgeCredentials.xml* a soubor se nachází ve vašem domovském adresáři stejně jako v souboru `MQMFTCredentials.xml` .

```
<tns:credentialsFile path="$HOME/ProtocolBridgeCredentials.xml" />
```

Stejně jako *MQMFTCredentails.xml*, můžete zašifrovat *ProtocolBridgeCredentials.xml* příkazem **fteObfuscate** . Pro účely dešifrování můžete uvést požadovanou cestu k souboru s klíči pověření pomocí přídavného prvku **credentialsKeyFile** , jak je zobrazeno v následujícím textu. Cesta může obsahovat proměnné prostředí.

```
<tns:credentialsKeyFile path="$HOME/CredKey.key"/>
```

Poznámka: Zadání hodnoty pro vlastnost agenta **agentCredentialsKeyFile** , vlastnost **commonCredentialsKeyFile** v `installation.properties`nebo přes systémovou vlastnost **com.ibm.wqmfte.cred.keyfile** nemá žádný vliv na hodnotu zadanou pro atribut **credentialsKeyFile** .

Podobně produkt Connect:Direct Bridge používá *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 identifikátor UID nebo PWD a další informace potřebné pro připojení k serveru Connect:Direct .

```
<tns:credentialsFile path="$HOME/ ConnectDirectCredentials.xml" />
```

Stejně jako soubor *ProtocolBridgeCredentials.xml* můžete zašifrovat soubor *ConnectDirectCredentials.xml* pomocí příkazu **fteObfuscate** . Pro účely dešifrování můžete uvést požadovanou cestu k souboru s klíči

pověření pomocí přídavného prvku **credentialsKeyFile** , jak je zobrazeno v následujícím textu. Cesta může obsahovat proměnné prostředí.

```
<tns:credentialsKeyFile path="$HOME/CredKey.key”/>
```

Poznámka: Zadání hodnoty pro vlastnost agenta **agentCredentialsKeyFile** , vlastnost **commonCredentialsKeyFile** v `installation.properties`nebo přes systémovou vlastnost **com.ibm.wqmfte.cred.keyfile** nemá žádný vliv na hodnotu zadanou pro atribut **credentialsKeyFile** .

Prvek **credentialsKeyFile** můžete zadat bez zadání prvku **credentialsFile** v souboru *ProtocolBridgeProperties.xml* .

Pokud nezadáte prvek **credentialsFile** , použije se výchozí soubor pověření *ProtocolBridgeCredentials.xml* agentem mostu protokolu a hodnota klíčového souboru zadaná v atributu **credentialsKeyFile** se použije k dešifrování souboru pověření.

Podobně můžete zadat prvek **credentialsKeyFile** bez určení prvku **credentialsFile** v souboru *ConnectDirectNodeProperties.xml* .

Pokud nezadáte prvek **credentialsFile** , použije se výchozí soubor pověření *ConnectDirectCredentials.xml* přemostění Connect:Direct a hodnota souboru s klíči zadaná v atributu **credentialsKeyFile** se použije k dešifrování souboru pověření.

Použití klíče z datové sady v systému z/OS

V systému z/OSmůžete zadat **MQMFTCredentials** a poskytnout soubor s klíči pověření pomocí PDSE. Viz téma “Konfigurace MQMFTCredentials.xml na systému z/OS” na stránce 563.

Související odkazy

Který příkaz MFT se připojuje ke správci front

Formát souboru pověření MFT

fteObfuscate (šifrovat citlivá data)

Ověřování připojení MFT a IBM MQ

Ověřování připojení umožňuje správci front být konfigurován pro ověřování aplikací pomocí poskytnutého ID uživatele a hesla. Má-li přidružený správce front povoleno zabezpečení a vyžaduje podrobnosti o pověření (ID uživatele a heslo), musí být funkce ověření připojení povolena před tím, než lze úspěšně vytvořit připojení ke správci front. Ověření připojení může být spuštěno v režimu kompatibility nebo v režimu ověření MQCSP.

Způsoby dodání údajů pověření

Mnoho příkazů Managed File Transfer podporuje následující metody dodání podrobností pověření:

Podrobnosti poskytnuté argumenty příkazového řádku.
Podrobnosti pověření lze zadat pomocí parametrů **-mquserid** a **-mqpassword** . Není-li **-mqpassword** zadán, je uživatel vyzván k zadání hesla, kde není vstup zobrazen.

Podrobnosti poskytnuté ze souboru pověření: `MQMFTCredentials.xml`.
Podrobnosti pověření mohou být předdefinovány v souboru `MQMFTCredentials.xml` buď jako prostý text, nebo zamlžené texty.

Informace o nastavení souboru MQMFTCredentials.xml na serveru IBM MQ for Multiplatforms viz “Konfigurace produktu MQMFTCredentials.xml na platformě Multiplatforms” na stránce 561.

Informace o nastavení souboru MQMFTCredentials.xml na serveru IBM MQ for z/OS viz “Konfigurace MQMFTCredentials.xml na systému z/OS” na stránce 563.

Přednost

Priorita pro určení podrobností pověření je:

1. Argument příkazového řádku.
2. Index `MQMFTCredentials.xml` podle přidruženého správce front a uživatele, který příkaz spouští.
3. `MQMFTCredentials.xml` index podle přidruženého správce front.
4. Výchozí režim zpětné kompatibility, v němž nejsou zadány žádné podrobnosti pověření, aby bylo možné povolit kompatibilitu s předchozími vydáními produktu IBM MQnebo IBM WebSphere MQ

Notes:

- Příkazy **`fteStartAgent`** a **`fteStartLogger`** nepodporují argument příkazového řádku **`-mquserid`**nebo **`-mqpassword`**a podrobnosti o pověření lze zadat pouze se souborem `MQMFTCredentials.xml` .
- z/OS

  V systému z/OSmusí být heslo uvedeno velkými písmeny, a to i v případě, že heslo uživatele má malá písmena. Je-li například heslo uživatele "password", bylo by třeba zadat jako "PASSWORD".

Související odkazy

Který příkaz MFT se připojuje ke správci front

Formát souboru pověření MFT

Konfigurace produktu `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 95. : 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

Tabulka 95. : Vlastnosti, které definují umístění souboru MQMFTCredentials.xml pro různé příkazy. (pokračování)		
Typ příkazu	**soubor vlastností**	**Název vlastnosti**
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 96. : 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.

V 9.2.0 V 9.2.0 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 564
Ověřování připojení modulu plug-in produktu IBM MQ Explorer MFT s koordinačním správcem front nebo správcem front příkazů a připojení k připojení agenta Managed File Transfer s koordinačním správcem front nebo správcem front příkazů lze spustit v režimu kompatibility nebo v režimu ověření MQCSP.

Související odkazy

Formát souboru pověření 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 97. : 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 98. : 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 produktu MQMFTCredentials.xml na platformě Multiplatforms” na stránce 561
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

Ověřování připojení modulu plug-in produktu IBM MQ Explorer MFT s koordinačním správcem front nebo správcem front příkazů a připojení k připojení agenta Managed File Transfer s koordinačním správcem front nebo správcem front příkazů lze spustit v režimu kompatibility nebo v režimu ověření MQCSP.

Informace o této úloze

Před IBM MQ 9.2.0je režim kompatibility výchozím nastavením pro ověření připojení. Výchozí režim kompatibility je však možné zakázat a povolit režim ověřování MQCSP.

V 9.2.0 V produktu IBM MQ 9.2.0je výchozím nastavením režim ověřování MQCSP.

Pro ověření připojení pro modul plug-in produktu 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 ověřování MQCSP. Zadáte-li při autorizaci pomocí režimu kompatibility heslo větší než 12 znaků, dojde k chybě a agent se neověří u správce front. Přečtěte si zprávu BFGAG0187E v tématu Diagnostické zprávy: BFGAG0001 - BFGAG9999.

Procedura

- Chcete-li vybrat režim ověření 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 **Podrobnosti o připojení-> Vlastnosti** .
  c) Klepněte na kartu **ID uživatele**.
  d) Ujistěte se, že je vybráno zaškrtávací políčko pro režim ověření připojení, které chcete použít:
  - V 9.1.0 Z produktu IBM MQ 9.1.0je zaškrtávací políčko **Režim kompatibility identifikace uživatele** standardně nezaškrtnuté. To znamená, že pokud je vybráno zaškrtávací políčko **Povolit identifikaci uživatele** , IBM MQ Explorer při připojování ke správci front použije ověření MQCSP. Pokud se produkt IBM MQ Explorer potřebuje připojit ke správci front pomocí režimu kompatibility místo ověření MQCSP, ujistěte se, že jsou zaškrtnuta políčka **Povolit identifikaci uživatele** i **Režim kompatibility identifikace uživatele** .
  - Před IBM MQ 9.1.0je standardně označeno zaškrtávací políčko **Režim kompatibility identifikace uživatele** . To znamená, že je-li zaškrtnuto políčko **Povolit identifikaci uživatele** , při připojování ke správci front bude produkt IBM MQ Explorer používat režim kompatibility. Pokud se produkt IBM MQ Explorer potřebuje připojit ke správci front pomocí ověření MQCSP, ujistěte se, že je označeno zaškrtávací políčko **Povolit identifikaci uživatele** a zrušte výběr zaškrtávacího políčka **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.

  Argument **useMQCSPAuthentication** má následující hodnoty:

  ano
  Režim ověření MQCSP se používá k ověření uživatele s použitím správce front.

  V 9.2.0 V produktu IBM MQ 9.2.0je výchozí hodnotou hodnota `true` . Pokud není zadán argument **useMQCSPAuthentication** , je standardně nastaven na hodnotu `true` a režim ověření MQCSP se používá k ověření uživatele se správcem front.

  ne
  Režim kompatibility se používá k ověřování identity uživatele se správcem front.

  Před IBM MQ 9.2.0, pokud parametr **useMQCSPAuthentication** není zadán, je standardně nastaven na hodnotu `false` a režim kompatibility se používá k ověření uživatele u správce front.

  Následující příklad ukazuje, 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 29
V produktu IBM MQ 8.0můžete odesílat hesla, která jsou zahrnuta do struktury MQCSP, buď chráněna, pomocí funkčnosti produktu IBM MQ , nebo šifrováním pomocí šifrování TLS.

Související odkazy

"Ověřování připojení MFT a IBM MQ" na stránce 560
Ověřování připojení umožňuje správci front být konfigurován pro ověřování aplikací pomocí poskytnutého ID uživatele a hesla. Má-li přidružený správce front povoleno zabezpečení a vyžaduje podrobnosti o pověření (ID uživatele a heslo), musí být funkce ověření připojení povolena před tím, než lze úspěšně vytvořit připojení ke správci front. Ověření připojení může být spuštěno v režimu kompatibility nebo v režimu ověření MQCSP.

Formát souboru pověření MFT

MFT pískoviště

Můžete omezit oblast systému souborů, ke které může agent přistupovat jako k části přenosu. Oblast, na kterou je agent omezen, se nazývá sandbox. Omezení můžete použít buď na agenta, nebo na uživatele, který požaduje přenos.

Sandboxy nejsou podporovány, je-li agent agentem mostu protokolu nebo agentem mostu Connect:Direct . Pro agenty, kteří potřebují přenášet data do front IBM MQ nebo z nich, nelze použít agenta sandboxing agenta.

Související odkazy

"Práce s pískovišti agenta MFT" na stránce 566
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 567
Můžete omezit oblast systému souborů, do níž lze soubory přenést, a z něj vychází jméno uživatele MQMD, které 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 přenášejí data do front produktu IBM MQ nebo z nich, nelze použít agenta sandboxing. Omezení přístupu k frontám IBM MQ pomocí pískovišť lze implementovat namísto použití uživatelského pískoviště, což je doporučené řešení pro případné požadavky na pískoviště. Další informace o uživatelském pískovišti naleznete v tématu "Práce s pískovišti uživatele MFT" na stránce 567 .

Chcete-li povolit agent sandboxing, 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.
- `!` je volitelný a uvádí, že následující hodnota pro *restricted_directory_name* je odepřena (vyloučena). Pokud `!` není zadán *restricted_directory_name* je povolená (zahrnutá) cesta.
- *separator* je oddělovač specifický pro danou platformu.

Chcete-li například omezit přístup, který má přístup AGENT1 pouze k adresáři `/tmp` , ale nedovolíte přístup k podadresáři `private` , nastavte vlastnost následujícím způsobem v souboru `agent.properties` patřícího do AGENT1: `sandboxRoot=/tmp:!/tmp/private`.

Vlastnost sandboxRoot je popsána v tématu Rozšířené vlastnosti agenta.

Agent i uživatel sandboxing nejsou podporovány na agentech mostu protokolu nebo na agentech mostu Connect:Direct .

Práce v sandboxu na platformách AIX, Linux, and Windows

ALW Na platformách AIX, Linux, and Windows umožňuje použití pískovišť, které adresáře Managed File Transfer Agent může číst a zapisovat do něj. Je-li aktivován sandbox, může Managed File Transfer Agent číst a zapisovat do adresářů uvedených jako povolené a všechny podadresáře, které uvedené adresáře obsahují, pokud nejsou podadresáře uvedeny jako odepřené v sandboxRoot. Managed File Transfer a sandbox nemá přednost před zabezpečením operačního systému. Uživatel, který spustil produkt Managed File Transfer Agent , musí mít přístup na úrovni operačního systému k libovolnému adresáři, který je schopen číst z adresáře nebo do něj zapisovat. Symbolický odkaz na adresář není následován, pokud adresář, na který se odkazuje, je mimo uvedené adresáře sandboxRoot (a podadresáře).

Práce v sandboxu v systému z/OS

z/OS V systému z/OSje v pískovišti omezován kvalifikátory názvů datové sady, ze kterých může Managed File Transfer Agent číst a zapisovat do něj. Uživatel, který spustil Managed File Transfer Agent , musí mít správné oprávnění k operačnímu systému pro všechny zahrnuté datové sady. Pokud uzavřete hodnotu kvalifikátoru názvu datové sady sandboxRoot do dvojitých uvozovek, bude hodnota následovat za běžnou konvencí z/OS a bude považována za plně kvalifikovanou. Pokud vynecháte dvojité uvozovky, bude předpona sandboxRoot opatřena předponou aktuálního ID uživatele. Pokud například nastavíte vlastnost sandboxRoot na následující: `sandboxRoot=//test`, agent může přistupovat k následujícím datovým sadám (ve standardní notaci z/OS) `//`*`username`*`.test.**` za běhu programu, pokud počáteční úrovně plně rozlišeného názvu datové sady neodpovídají sandboxRoot, požadavek na přenos je odmítnut.

Práce v pískovišti v systémech IBM i

IBM i U souborů v integrovaném systému souborů v systémech IBM i umožňuje použití pískoviště a zápisu do nich adresáře, které adresář Managed File Transfer Agent může číst a zapisovat. Je-li aktivován sandbox, může Managed File Transfer Agent číst a zapisovat do adresářů uvedených jako povolené a všechny podadresáře, které uvedené adresáře obsahují, pokud nejsou podadresáře uvedeny jako odepřené v sandboxRoot. Managed File Transfer a sandbox nemá přednost před zabezpečením operačního systému. Uživatel, který spustil produkt Managed File Transfer Agent , musí mít přístup na úrovni operačního systému k libovolnému adresáři, který je schopen číst z adresáře nebo do něj zapisovat. Symbolický odkaz na adresář není následován, pokud adresář, na který se odkazuje, je mimo uvedené adresáře sandboxRoot (a podadresáře).

Související odkazy

“Další kontroly pro přenosy pomocí zástupných znaků” na stránce 570
Pokud byl agent konfigurován s uživatelem nebo sandboxem agenta, abyste omezili umístění, do kterých může agent přenášet soubory, můžete uvést, že se mají provést další kontroly na přenosech zástupného znaku pro daného agenta.

“Práce s pískovišti agenta MFT” na stránce 566
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 níž lze soubory přenést, a z něj vychází jméno uživatele MQMD, které požaduje přenos.

Uživatelská pískoviště nejsou podporována, je-li agent agentem mostu protokolu nebo agentem mostu Connect:Direct .

Chcete-li povolit uživatelské sandbox, přidejte do souboru `agent.properties` pro agenta následující vlastnost, kterou 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 částí systému souborů, k nimž má uživatel, který požaduje přenos, přístup.

XML `UserSandboxes.xml` se skládá z prvku <agent> , který obsahuje nula nebo více prvků <sandbox> . Tyto prvky popisují, která pravidla se používají ke kterým uživatelům. Atribut `user` prvku <sandbox> je vzorek, který se používá k porovnání s uživatelem MQMD požadavku.

Soubor `UserSandboxes.xml` je pravidelně znovu načten agentem a veškeré platné změny souboru ovlivní chování agenta. Výchozí interval nového načtení je 30 sekund. Tento interval lze změnit zadáním vlastnosti agenta xmlConfigReloadInterval v souboru `agent.properties` .

Pokud zadáte atribut nebo hodnotu `userPattern="regex"` , bude atribut `user` interpretován jako regulární výraz Java . Další informace viz Regulární výrazy používané MFT.

Pokud nezadáte atribut `userPattern="regex"` nebo hodnotu, atribut `user` se interpretuje jako vzor s následujícími zástupnými znaky:

- hvězdička (*), která představuje nula nebo více znaků
- otazník (?), který představuje právě jeden znak

Shody se provádějí v pořadí, ve kterém jsou prvky <sandbox> uvedeny v souboru. Použije se pouze první shoda, všechny následující potenciální shody v souboru se ignorují. Pokud žádný z prvků <sandbox> uvedený v souboru neodpovídá uživateli MQMD přidruženému ke zprávě požadavku na přenos, přenos nebude mít přístup k systému souborů. Pokud byla nalezena shoda mezi jménem uživatele produktu MQMD a atributem `user` , odpovídá tato shoda sadu pravidel uvnitř prvku produktu <sandbox> , který se použije na přenos. Tato sada pravidel se používá k určení, které souborynebo datové sady lze číst z nebo do přenosu jako část 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 není oprávněn provádět žádné čtení nebo zápisy.

Poznámka: Prvek <read> musí být před prvkem <write> a prvek <include> musí být před prvkem <exclude> , a to 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 může být přenesen. Tyto vzory lze zadat pomocí prvků <include> a <exclude> . Atribut `name` prvku <include> nebo <exclude> určuje vzor, pro který má být porovnávána shoda. Nepovinný atribut `type` určuje, zda je hodnota názvu vzorem souboru nebo fronty. Není-li atribut `type` zadán, bude agent považovat vzor za soubor nebo cestu k 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 soubory, datové sady, nebo fronty lze číst nebo zapisovat do. Operace je povolena, pokud se kanonická cesta k souboru, datová sada, nebo název fronty shoduje alespoň s jedním ze zahrnutých vzorů a přesně nula z vylučovací vzory. Vzory určené pomocí atributu `name` v prvcích <include> a <exclude> používají oddělovače cesty a konvence odpovídající platformě, na které agent běží. Určíte-li relativní cesty k souboru, budou cesty vyřešeny vzhledem k vlastnosti `transferRoot` agenta.

Při zadávání omezení fronty je podporována syntaxe parametru QUEUE@QUEUEMANAGER s následujícími pravidly:

- Pokud ve znaku chybí znak (@), bude tento vzorek považován za název fronty, ke kterému lze přistupovat v libovolném správci front. Pokud je vzor například `name` , zachází se se stejným způsobem jako s `name@**`.
- Je-li znak at (@) prvním znakem v dané položce, bude vzor považován za název správce front a lze k němu přistupovat všechny fronty ve správci front. Pokud je vzor například `@name` , zachází se se stejným způsobem jako s `**@name`.

Následující zástupné znaky mají speciální význam, když je uvedete jako část atributu `name` prvků `<include>` a `<exclude>` :

*****
: Jedna hvězdička odpovídá žádnému nebo více znakům v názvu adresáře, nebo v kvalifikátoru názvu fronty název datové sady nebo .

?
: Otazník odpovídá přesně jednomu znaku v názvu adresáře nebo v kvalifikátoru názvu fronty název datové sady nebo .

******
: Dvě hvězdičky se shodují s žádným nebo více názvy adresářů, nebo s více kvalifikátory v názvu datové sady nebo názvu fronty. Také cesty, které končí oddělovačem cesty, mají implicitní "**" přidané na konec cesty. Takže `/home/user/` je stejné jako `/home/user/**`.

Příklad:

- `/**/test/**` odpovídá libovolnému souboru, který má ve své cestě adresář `test`
- `/test/file?` odpovídá libovolnému souboru uvnitř adresáře `/test` , který začíná řetězcem `file` , za nímž následuje libovolný znak.
- `c:\test\*.txt` odpovídá libovolnému souboru uvnitř adresáře `c:\test` s příponou `.txt`
- `c:\test\**\*.txt` odpovídá libovolnému souboru uvnitř adresáře `'c:\test` nebo jednomu z jeho podadresářů, který má příponu `.txt`
- z/OS `//'TEST.*.DATA'` odpovídá jakékoliv datové sadě, která má první kvalifikátor TEST, má jakýkoli druhý kvalifikátor a třetí kvalifikátor DATA.
- *@QM1 odpovídá libovolné frontě ve správci front QM1 , který má jediný kvalifikátor.
- Produkt `TEST.*.QUEUE@QM1` odpovídá libovolné frontě ve správci front QM1 , který 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` , je třeba plně vyřešit určením pevných odkazů v prvcích `<include>` a `<exclude>` . Máte-li například symbolický odkaz tam, kde je `/var` mapuje na `/SYSTEM/var`, musíte zadat tuto cestu jako `<tns:include name="/SYSTEM/var"/>`, jinak se zamýšlený přenos nezdaří s chybou zabezpečení prostředí sandbox uživatele.

Příklad

Tento příklad ukazuje, jak povolit uživateli s názvem uživatele MQMD `guest` přenést jakýkoli soubor z adresáře `/home/user/public` nebo jeho podadresářů v 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 povolit kterémukoli uživateli s názvem uživatele MQMD `account` následovaným jedinou číslicí, například `account4`, k provedení následujících akcí:

- Přeneste libovolný soubor z adresáře `/home/account` nebo z jeho podadresářů, kromě adresáře `/home/account/private` na systému, kde je spuštěn agent AGENT_SATURN
- Přeneste jakýkoli soubor do adresáře `/home/account/output` nebo do libovolného z jeho podadresářů v systému, kde je spuštěn agent AGENT_SATURN
- Přečtěte si zprávy z front v lokálním správci front, které začínají předponou `ACCOUNT.` , pokud nezačne s `ACCOUNT.PRIVATE.` (který má `PRIVATE` na druhé úrovni).
- Přenést data do front začínajících předponou `ACCOUNT.OUTPUT.` na libovolném správci front.

To allow a user with the MQMD user name `account` to complete these actions, add the following `<sandbox>` element to the file `UserSandboxes.xml`, in AGENT_SATURN's configuration directory:

```
<?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 pomocí zástupných znaků” na stránce 570
Pokud byl agent konfigurován s uživatelem nebo sandboxem agenta, abyste omezili umístění, do kterých může agent přenášet soubory, můžete uvést, že se mají provést další kontroly na přenosech zástupného znaku pro daného agenta.

Soubor MFT `agent.properties`

Další kontroly pro přenosy pomocí zástupných znaků

Pokud byl agent konfigurován s uživatelem nebo sandboxem agenta, abyste omezili umístění, do kterých může agent přenášet soubory, můžete uvést, že se mají provést další kontroly na přenosech zástupného znaku pro daného agenta.

Vlastnost produktu additionalWildcardSandboxChecking

Chcete-li povolit další kontrolu pro přenosy pomocí zástupných znaků, 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 o čtení umístění, které je mimo definované pískoviště pro hledání shody souborů se zástupným znakem, dojde k selhání přenosu. Je-li v rámci jednoho požadavku na přenos více přenosů a jeden z těchto požadavků selže kvůli pokusu o načtení umístění mimo sandbox, celý přenos se nezdaří. Pokud kontrola selže, je příčina selhání uvedena v chybové zprávě.

Je-li vlastnost additionalWildcardSandboxChecking vynechána ze souboru `agent.properties` agenta nebo je nastavena na hodnotu false, nejsou prováděny žádné další kontroly pro přenosy pomocí zástupných znaků pro tohoto agenta.

Chybové zprávy pro kontrolu zástupného znaku

Zprávy, které jsou hlášeny při požadavku na přenos se zástupnými znaky na umístění mimo konfigurované umístění sandboxu, jsou následující.

K následující zprávě dojde, když se cesta k souboru se zástupnými znaky v požadavku na přenos nachází mimo omezené pískoviště:

```
BFGSS0077E: Pokus o čtení cesty k souboru: cesta byl odepřen.
Cesta k souboru je umístěna mimo omezené přenosové prostředí sandbox.
```

Pokud přenos v rámci více požadavků na přenos obsahuje požadavek na přenos se zástupnými znaky, je-li cesta umístěna mimo omezené pískoviště, dojde k následující zprávě:

```
BFGSS0078E: Pokus o čtení cesty k souboru: path byl ignorován jako jiný přenos
položka ve spravovaném přenosu se pokusila číst mimo omezené přenosové prostředí sandbox.
```

K následující zprávě dojde, když je soubor umístěn mimo omezené pískoviště:

```
BFGSS0079E: Pokus o čtení souboru cesta k souboru byl odepřen.
Soubor je umístěn mimo omezené přenosové prostředí sandbox.
```

Následující zpráva se vyskytuje ve více požadavcích na přenos, kde další požadavek na přenos zástupného znaku způsobil, že tento požadavek byl ignorován:

```
BFGSS0080E: Pokus o čtení souboru: cesta k souboru byla ignorována jako další přenos.
položka ve spravovaném přenosu se pokusila číst mimo omezené přenosové prostředí sandbox.
```

V případě jednotlivých přenosů souborů, které nezahrnují zástupné znaky, se zpráva, která se ohlásí, když přenos zahrnuje soubor, který je umístěn mimo sandbox, beze změny ze starších verzí:

```
Došlo k 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 567
Můžete omezit oblast systému souborů, do níž lze soubory přenést, a z něj vychází jméno uživatele MQMD, které požaduje přenos.

“Práce s pískovišti agenta MFT” na stránce 566
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 zabezpečení SSL nebo TLS pro produkt MFT

Protokol SSL nebo TLS lze použít s produktem IBM MQ Managed File Transfer k zabezpečení komunikace mezi agenty a jejich správci front agentů, příkazy a správci front, ke kterým se připojují, a různým správcem front k připojení správce front v rámci vaší topologie.

Než začnete

Šifrování SSL nebo TLS můžete použít k šifrování zpráv, které proudí přes topologii produktu IBM MQ Managed File Transfer . Patří k nim:

- Zprávy, které procházejí mezi agentem a jeho správcem front agenta.
- Zprávy pro příkazy a správce front, ke kterým se připojují.
- Interní zprávy, které vedou mezi správci front agentů, správci front příkazů a koordinačním správcem front v rámci topologie.

Informace o této úloze

Obecné informace o použití SSL s produktem IBM MQviz “Práce s protokolem SSL” na stránce 268.
V produktu IBM MQ je Managed File Transfer standardní klientskou aplikací produktu Java .

Chcete-li používat SSL s produktem Managed File Transfer, postupujte takto:

Postup

1. Vytvořte soubor úložiště údajů o důvěryhodnosti a volitelně soubor úložiště klíčů (tyto soubory mohou být stejného souboru). Pokud nepotřebujete ověření klienta (to znamená SSLCAUTH=OPTIONAL on channels), nemusíte poskytovat úložiště klíčů. Požadujete úložiště údajů o důvěryhodnosti pouze pro ověření certifikátu správce front.

   Algoritmus klíče použitý pro vytvoření certifikátů pro úložiště údajů o důvěryhodnosti a úložiště klíčů musí být RSA pro práci s IBM MQ.
2. Nastavte správce front produktu IBM MQ tak, aby používal zabezpečení SSL.

   Informace o nastavení správce front pro použití zabezpečení SSL s použitím produktu IBM MQ Explorer viz například téma Konfigurace zabezpečení SSL pro správce front.
3. Uložte soubor úložiště údajů o důvěryhodnosti a soubor úložiště klíčů (pokud jej máte) ve vhodném umístění. Navrhovaným umístěním je adresář *config_directory*/*coordination_qmgr*/agents/*agent_name* .
4. Nastavte vlastnosti zabezpečení SSL, které jsou vyžadovány pro každého správce front s povoleným SSL v odpovídajícím souboru vlastností produktu Managed File Transfer . Každá sada vlastností odkazuje na samostatného správce front (agenta, koordinace 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 SSL. Jak vlastnosti **CipherSpec** , tak **CipherSuite** jsou poskytovány z důvodu terminologických rozdílů mezi IBM MQ a Java. Produkt Managed File Transfer přijímá buď vlastnost a provádí nezbytný převod, takže nemusíte nastavovat obě vlastnosti. Pokud zadáte obě vlastnosti **CipherSpec** nebo **CipherSuite** , bude mít přednost **CipherSpec** .

   Vlastnost **PeerName** je volitelná. Tuto vlastnost můžete nastavit na rozlišující název správce front, k němuž se chcete připojit. Managed File Transfer odmítá připojení k chybnému serveru SSL s rozlišujícím názvem, který se neshoduje.

   Nastavte vlastnosti **SslTrustStore** a **SslKeyStore** na názvy souborů, které odkazují na úložiště údajů o důvěryhodnosti a soubory úložiště klíčů. Pokud nastavujete tyto vlastnosti pro agenta, který je již spuštěný, zastavte a restartujte agenta, abyste se znovu připojili v režimu SSL.

   Soubory vlastností obsahují nešifrovaná hesla, takže zvažte nastavení příslušných oprávnění systému souborů.

   Další informace o vlastnostech SSL viz “Vlastnosti SSL/TLS pro MFT” na stránce 573.
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 nebudete moci publikovat existenci agenta do koordinačního správce front.

b) Upravte soubor `agent.properties` , který byl vytvořen předchozím krokem, a přidejte informace o zabezpečení SSL. Když je agent úspěšně spuštěn, provede se pokus o publikaci znovu.

6. Pokud jsou spuštění agenti nebo instance produktu IBM MQ Explorer, zatímco se změní vlastnosti SSL v souboru `agent.properties` nebo `coordination.properties` , je třeba restartovat agenta nebo IBM MQ Explorer.

Související odkazy

Soubor MFT `agent.properties`

Vlastnosti SSL/TLS pro MFT

Některé soubory vlastností produktu MFT zahrnují vlastnosti SSL a TLS. Můžete použít SSL nebo TLS s IBM MQ a Managed File Transfer , chcete-li zabránit neautorizovaným připojením mezi agenty a správci front, a šifrovat přenos zpráv mezi agenty a správci front.

Následující soubory vlastností produktu MFT obsahují 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`

Informace o použití SSL nebo TLS s produktem Managed File Transfernaleznete v tématu Konfigurace šifrování SSL nebo TLS pro produkt MFT.

V produktu IBM WebSphere MQ 7.5můžete použít proměnné prostředí v některých vlastnostech produktu Managed File Transfer , které představují umístění souborů nebo adresářů. To umožňuje umístění souborů nebo adresářů, které se používají při spouštění částí produktu, aby se lišily v závislosti na změnách prostředí, jako např. který uživatel spouští proces. Další informace naleznete v tématu Použití proměnných prostředí ve vlastnostech produktu MFT.

Připojení ke správci front v režimu klienta s ověřením kanálu

Produkt IBM WebSphere MQ 7.1 zavedl autentizační záznamy kanálu k řízení přesnějšího přístupu na úrovni kanálu. Tato změna v chování znamená, že standardně nově vytvořený produkt IBM WebSphere MQ 7.1 nebo pozdější správci front odmítne připojení klienta z komponenty Managed File Transfer .

Další informace o ověření kanálu viz “Záznamy ověření kanálu” na stránce 47.

Pokud konfigurace ověření kanálu pro SVRCONN používaného produktem Managed File Transfer určuje neprivilegované ID MCAUSER, je třeba pro správce front, fronty a témata udělit určité záznamy oprávnění, které umožní správné fungování produktu Managed File Transfer Agent a příkazů. Použijte příkaz MQSC SET CHLAUTH nebo PCF Nastavit záznam ověření kanálu k vytvoření, úpravě nebo odebrání záznamů ověření kanálu. Pro všechny agenty Managed File Transfer , které chcete připojit ke správci front produktu IBM WebSphere MQ 7.1 nebo novější, můžete buď nastavit ID MCAUSER pro použití pro všechny agenty, nebo nastavit samostatné ID MCAUSER pro každého agenta.

Udělte každému ID MCAUSER následující oprávnění:

- Záznamy oprávnění vyžadované pro správce front:
  - connect
  - setid
  - inq
- Záznamy oprávnění požadované pro fronty.

  Pro všechny fronty specifické pro agenta, které jsou názvy front, které končí v *název_agenta* v následujícím seznamu, musíte vytvořit tyto záznamy oprávnění fronty pro každého agenta, kterého se chcete připojit ke správci front produktu IBM WebSphere MQ 7.1 nebo novější pomocí připojení klienta.

  - put, get, dsp (SYSTEM.DEFAULT.MODEL.QUEUE)

  - put, get, setid, browse (SYSTEM.FTE.COMMAND.*název_agenta*)
  - put, get (SYSTEM.FTE.DATA.*název_agenta*)
  - put, get (SYSTEM.FTE.REPLY.*název_agenta*)
  - put, get, inq, browse (SYSTEM.FTE.STATE.*název_agenta*)
  - put, get, browse (SYSTEM.FTE.EVENT.*název_agenta*)
  - put, get (SYSTEM.FTE)
- Záznamy oprávnění požadované pro témata:
  - sub, pub (SYSTEM.FTE)
- Záznamy oprávnění požadované pro přenosy souborů.

  Pokud máte oddělené ID MCAUSER pro zdrojový a cílový agent, vytvořte záznamy oprávnění ve frontách agentů na zdroji i cíli.

  Například, je-li ID MCAUSER zdrojového agenta **user1** a ID cílového agenta MCAUSER ID je **user2**, nastavte následující oprávnění pro uživatele agenta:

Uživatel AGENT	Fronta	Požadované oprávnění
user1	SYSTEM.FTE.DATA.*název_cíl_cíle*	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 produktu Connect:Direct

Konfigurujte agenta mostu Connect:Direct a uzel produktu Connect:Direct pro připojení k sobě prostřednictvím protokolu SSL vytvořením úložiště klíčů a úložiště údajů o důvěryhodnosti a nastavením vlastností v souboru vlastností agenta mostu Connect:Direct .

Informace o této úloze

Tento postup obsahuje pokyny pro získání klíčů podepsaných certifikačních autorit. Pokud nepoužíváte certifikační autoritu, můžete vygenerovat certifikát podepsaný svým držitelem. Další informace o generování certifikátu podepsaného (svým) držitelem viz “Práce s SSL/TLS v AIX, Linux, and Windows” na stránce 279.

Tyto kroky zahrnují pokyny pro vytvoření nového úložiště klíčů a úložiště údajů o důvěryhodnosti pro agenta mostu Connect:Direct . Pokud má agent mostu Connect:Direct již úložiště klíčů a úložiště údajů o důvěryhodnosti, které používá k bezpečnému připojení ke správci front produktu IBM MQ , můžete použít existující úložiště klíčů a úložiště údajů o důvěryhodnosti při zabezpečeném připojení k uzlu produktu Connect:Direct . Další informace naleznete v části “Konfigurace zabezpečení SSL nebo TLS pro produkt MFT” na stránce 571.

Postup

Pro uzel Connect:Direct proveďte následující kroky:

1. Vygenerujte klíč a podepsaný certifikát pro uzel Connect:Direct .

   To můžete provést pomocí nástroje správy klíčů produktu IBM , který je dodáván s produktem IBM MQ. Další informace viz téma “Práce s protokolem SSL” na stránce 268.
2. Odešlete požadavek na certifikační autoritu, aby byl podepsán klíč. Vrátíte se k vrácení certifikátu.
3. Vytvořte textový soubor, například `/test/ssl/certs/CAcert`, který obsahuje veřejný klíč certifikačního orgánu.

4. Nainstalujte volbu Secure + Option na uzel Connect:Direct .

   Pokud uzel již existuje, můžete volbu Secure + Option nainstalovat opětovným spuštěním instalačního programu, zadáním umístění existující instalace a výběrem volby Instalovat pouze produkt Secure +.
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 souboru `/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+50hTKI8OGvBvWXO4fHyvIX5aslwhBoArXIS1AtNTrptPvoaP1zyIAeZ6OCVo/
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.

   - V systému AIX and Linux spusťte příkaz **spadmin.sh**.
   - V systémech Windows klepněte na volbu **Start** > **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 ikonu **.Lokální** linka pro úpravu hlavního nastavení SSL nebo TLS.

   a) Vyberte volbu **Povolit protokol SSL** nebo **Povolit protokol TLS**v závislosti na tom, jaký protokol používáte.

   b) Vyberte volbu **Zakázat přepis**.

   c) Vyberte alespoň jednu šifrovací sadu.

   d) Chcete-li dvousměrné ověření, změňte hodnotu volby **Povolit ověření klienta** na Yes.

   e) Do pole **Důvěryhodný kořenový certifikát** zadejte cestu k souboru veřejného certifikátu certifikační autority, `/test/ssl/certs/CAcert`.

   f) Do pole **Soubor certifikátu klíčů** zadejte cestu k souboru, který jste vytvořili, `/test/ssl/cd/keyCertFile/`*node_name*`.txt`.
9. Poklepejte na **.Klient** řádek pro úpravu hlavního nastavení SSL nebo TLS.

a) Vyberte volbu **Povolit protokol SSL** nebo **Povolit protokol TLS**v závislosti na tom, jaký protokol používáte.

b) Vyberte volbu **Zakázat přepis**.

Pro agenta mostu Connect:Direct proveďte následující kroky:

10. Vytvořte úložiště údajů o důvěryhodnosti. To lze provést vytvořením prázdného 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 do souboru následující řádky:

    ```
    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 vytvoření úložiště údajů o důvěryhodnosti.

13. Chcete-li dvousměrné 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) Generujte 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 do souboru následující řádky:

    ```
    cdNodeKeystore=/test/ssl/fte/stores/keystore.jks
    cdNodeKeystorePassword=password
    ```

V příkladu v tomto kroku je heslo *password* heslo, které jste zadali při vytváření úložiště klíčů.

Související úlohy

Konfigurace mostu produktu Connect:Direct

ALW Zabezpečení klientů AMQP

Zabezpečte připojení klientů AMQP pomocí řady mechanizmů zabezpečení a zajistěte, aby byla data vhodně chráněna v síti. Zabezpečení můžete sestavovat do aplikací produktu MQ Light . Můžete také použít existující funkce zabezpečení produktu IBM MQ s klienty AMQP stejným způsobem, jako jsou funkce použity pro jiné aplikace.

Pravidla ověření kanálu (CHLAUTH)

Můžete použít pravidla ověření kanálu k omezení připojení TCP ke správci front. Kanály AMQP podporují použití pravidel pro ověřování kanálu, které jste nakonfigurovali pro správce front. Jsou-li pravidla ověřování kanálu definována s profilem, který odpovídá libovolnému kanálu AMQP ve správci front, budou tato pravidla použita pro tyto kanály. Při výchozím nastavení je ověřování kanálu povoleno u nových správců front produktu IBM® MQ , takže je třeba před použitím kanálu AMQP dokončit alespoň nějakou konfiguraci.

Další informace o tom, jak konfigurovat pravidla ověřování kanálu pro povolení připojení AMQP k vašemu správci front, najdete v tématu Vytvoření a použití kanálů AMQP.

Ověření připojení (CONNAUTH)

Pro ověření připojení ke správci front můžete použít ověření připojení. Kanály AMQP podporují použití ověření připojení pro řízení přístupu ke správci front z aplikací AMQP.

Protokol AMQP používá rámec SASL (Simple Authentication and Security Layer) k určení, jak je připojení ověřováno. K dispozici jsou různé mechanizmy SASL a IBM MQ podporuje dva mechanismy SASL: ANONYMOUS a PLAIN.

V případě ANONYMOUS nebyla z klienta do správce front pro ověření předávána žádná pověření. Pokud má objekt MQ AUTHINFO uvedený v atributu CONNAUTH hodnotu CHCKCLNT nebo REQDADM (pokud se připojuje jako administrativní uživatel), připojení se odmítne. Je-li hodnota CHCKCLNT NONE nebo OPTIONAL, připojení je akceptováno.

V případě služby PLAIN je pro ověření předáno jméno uživatele a heslo z klienta do správce front. Pokud má objekt MQ AUTHINFO uvedený v atributu CONNAUTH hodnotu CHCKCLNT, je hodnota NONE, připojení odmítnuto. Je-li hodnota parametru CHCKCLNT VOLITELNÁ, POŽADOVÁNO nebo REQDADM (pokud se připojuje jako administrativní uživatel), je správce front ověřován jménem uživatele a heslem. Správce front zkontroluje operační systém (je-li objekt AUTHINFO typu IDPWOS) nebo úložiště LDAP (je-li objekt AUTHINFO typu IDPWLDAP).

Následující tabulka shrnuje toto chování ověření:

Tabulka 99. Souhrn mechanizmů SASL a ověření připojení

Mechanizmus SASL	**Pověření předávaná z klienta do správce front?**	**hodnota CHKCLNT**
anonymní	Ne	REQUIRED nebo REQDADM-připojení odmítnuto NONE nebo OPTIONAL-připojení přijato

Tabulka 99. Souhrn mechanizmů SASL a ověření připojení (pokračování)		
Mechanizmus SASL	**Pověření předávaná z klienta do správce front?**	**hodnota CHKCLNT**
Obyčejné	Ano, jméno uživatele a heslo	REQUIRED, REQDADM nebo OPTIONAL-jméno uživatele a heslo zkontrolované správcem front NONE-odmítnuto připojení

Pokud používáte klienta MQ Light , můžete zadat pověření tak, že je zahrnete 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 produktu IBM MQ , pod kterým jsou všechna připojení k příslušnému kanálu autorizována. Všechna připojení z klientů AMQP do tohoto kanálu přebírají ID MCAUSER, které jste nakonfigurovali. Toto ID uživatele se používá pro ověřování systému zpráv v různých tématech.

Chcete-li zabezpečit připojení ke správcům front, doporučuje se použít ověření kanálu (CHLAUTH). Používáte-li ověřování kanálu, doporučuje se konfigurovat hodnotu MCAUSER na neprivilegovaného uživatele. Tím je zajištěno, že pokud připojení ke kanálu neodpovídá pravidlu CHLAUTH, nebude připojení povoleno provádět žádné zprávy ve správci front.

Poznámka: Windows V systému Windowsje před IBM MQ 9.1.1podporováno nastavení ID uživatele MCAUSER pouze pro ID uživatelů o délce až 12 znaků. V 9.2.0 Z IBM MQ 9.1.1 Continuous Deliverya z IBM MQ 9.2.0 Long Term Supportse odstraní limit 12 znaků.

Podpora šifrování protokolu

Kanály AMQP podporují šifrování SSL/TLS pomocí klíčů z úložiště klíčů nakonfigurovaného pro vašeho správce front. Volby konfigurace kanálu AMQP pro šifrování SSL/TLS podporují stejné volby jako jiné typy kanálu MQ ; můžete zadat specifikaci šifry a to, zda správce front vyžaduje certifikáty z připojení klienta AMQP.

Pomocí atributů standardu FIPS správce front můžete řídit sady šifer SSL/TLS, které lze použít k zabezpečení připojení z klientů AMQP.

Informace o tom, jak nastavit úložiště klíčů pro správce front, najdete v tématu Práce s SSL nebo TLS na systémech UNIX, Linux a Windows.

Informace o tom, jak nakonfigurovat podporu SSL/TLS pro připojení klienta AMQP, najdete v tématu Vytvoření a použití kanálů AMQP.

Java Authentication and Authorization Service (JAAS)

Volitelně můžete nakonfigurovat kanály AMQP pomocí přihlašovacího modulu JAAS , který může zkontrolovat jméno uživatele a heslo zadané klientem AMQP. Viz “Konfigurování služby JAAS pro kanály AMQP” na stránce 579.

Související úlohy

Vyvíjení klientských aplikací AMQP

Vytvoření a použití kanálů AMQP

ALW Omezení převzetí klienta AMQP

Je-li vytvořeno připojení klienta AMQP, které má stejný identifikátor klienta jako existující připojení klienta AMQP, bude při výchozím nastavení odpojeno existující připojení klienta. Správce front však můžete nakonfigurovat tak, aby omezoval chování převzetí klienta tak, aby převzetí bylo možné pouze v případě, že jsou splněna určitá kritéria.

Například odpojení existujícího připojení klienta nemusí být vhodné, pokud existují aplikace AMQP vyvíjeny různými týmy a že 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).

Použijte nastavení atributů správce front **AdoptNewMCA** a **AdoptNewMCACheck** k uvedení požadované úrovně omezení převzetí klienta, jak je podrobně uvedeno v následující tabulce:

*Tabulka 100. Nastavení **AdoptNewMCA** a **AdoptNewMCACheck** pro omezení převzetí klienta*

AdoptNewMCA	AdoptNewMCACheck	Kritéria zkontrolovaná před povolením převzetí klienta
NO nebo nedefinováno	Nelze použít	Není. Převzetí klienta je povoleno pro všechna ověření klienta, která jsou ověřena a předávají všechna pravidla CHLAUTH.
ALL (nebo hodnota jiná než NO)	QM nebo nedefinováno	Není. Převzetí klienta je povoleno pro všechna ověření klienta, která jsou ověřena a předávají všechna pravidla CHLAUTH.
ALL (nebo hodnota jiná než NO)	NAME	ID uživatele (je-li SASL povoleno) Název kanálu
ALL (nebo hodnota jiná než NO)	ADDRESS	ID uživatele (je-li SASL povoleno) Adresa IP
ALL (nebo hodnota jiná než NO)	ALL	ID uživatele (je-li SASL povoleno) Název kanálu Adresa IP

Atributy správce front **AdoptNewMCA** a **AdoptNewMCACheck** jsou součástí konfigurace správce front, která je definována ve stanze CHANNELS. V systémech IBM MQ pro systémy Windows a IBM MQ pro systémy Linux x86-64 upravte informace o konfiguraci pomocí konzoly IBM MQ Explorer. V jiných systémech upravte informace úpravou konfiguračního souboru `qm.ini` . Informace o tom, jak upravit informace o kanálech správce front, naleznete v tématu Atributy kanálů.

Související úlohy

Vyvíjení klientských aplikací AMQP

Vytvoření a použití kanálů AMQP

ALW Konfigurování služby JAAS pro kanály AMQP

Vlastní moduly služby JAAS (Java Authentication and Authorization Service) lze použít k ověření jména uživatele a pověření hesla předávaných klientovi AMQP pomocí klienta AMQP při připojování.

Informace o této úloze

Možná budete chtít použít vlastní modul JAAS , pokud již používáte moduly JAAS pro ověřování v jiných systémech založených na jazyku Java a chcete znovu použít tyto moduly pro ověření připojení AMQP

k produktu MQ. Případně můžete chtít napsat vlastní modul JAAS , pokud funkce ověření 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 ověření připojení AMQP ke správci front, bude modul použit pro všechny kanály AMQP. Název kanálu, který vyvolal modul JAAS , je předán modulu, což vám umožňuje kódovat různé protokoly JAAS v chování pro různé kanály.

Další informace jsou také předány modulu JAAS :

- ID klienta klienta AMQP, který se pokouší o ověření.
- Síťová adresa klienta AMQP.
- Název kanálu, který vyvolal modul JAAS .

Postup

Konfigurační modul JAAS pro kanály AMQP nakonfigurujete provedením následujících kroků:

1. Definujte soubor `jaas.config` obsahující jednu nebo více sekcí konfigurace modulu JAAS . Stanza musí určovat úplný název třídy Java, která implementuje rozhraní JAAS `javax.security.auth.spi.LoginModule` .
   - Výchozí soubor `jaas.config` se dodává spolu s produktem a je umístěn v *QM_data_directory*/`amqp/jaas.config`.
   - Předkonfigurovaný oddíl s názvem `MQXRConfig` je již definován ve výchozím souboru `jaas.config` .
2. Zadejte název oddílu, který 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 tento tvar:

   ```
   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 ve stanze konfigurace JAAS .

   To provedete tak, že přidáte cestu ke třídě JAAS do souboru `service.env` produktu MQ . 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 se dodává spolu s produktem v adresáři *mq_installation_directory*/`amqp/samples` . Ukázkový přihlašovací modul JAAS ověřuje všechna připojení klientů bez ohledu na jméno uživatele nebo heslo, se kterým se klient připojuje.

Zdrojový kód ukázky můžete upravit a znovu jej zkompilovat, chcete-li se pokusit o ověření pouze určitých uživatelů s konkrétním heslem. Chcete-li nakonfigurovat kanál AMQP v systému UNIX pro použití ukázkového přihlašovacího modulu JAAS dodaného 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 zkoušíte ukázkový modul, nejsou vyžadovány žádné změny produktu `jaas.config` .

Související úlohy

Vyvíjení klientských aplikací AMQP

Vytvoření a použití kanálů AMQP

Advanced Message Security

Advanced Message Security (AMS) je komponenta produktu IBM MQ , která poskytuje vysokou úroveň ochrany citlivých dat procházejících přes síť IBM MQ , a to bez dopadu na koncové aplikace.

Přehled produktu Advanced Message Security

Aplikace produktu IBM MQ mohou používat produkt Advanced Message Security k odesílání citlivých dat, jako jsou například finanční transakce s vysokou hodnotou a osobní informace, s různými úrovněmi ochrany s použitím modelu šifrování pomocí veřejného klíče.

Související odkazy

Návratové kódy GSKit použité ve zprávách produktu AMS

Vlastnosti a funkce produktu Advanced Message Security

Advanced Message Security rozšiřuje služby zabezpečení produktu IBM MQ tak, aby poskytovaly data pro podepisování a šifrování dat na úrovni zpráv. Rozbalená služba zaručuje, že data zprávy nebyla upravena mezi okamžikem, kdy byla původně vložena do fronty, a když je načtena. Kromě toho produkt AMS ověřuje, zda je odesilatel dat zpráv autorizován k vložení podepsaných zpráv do cílové fronty.

Produkt AMS poskytuje následující funkce:

- Zabezpečuje citlivé nebo vysoce hodnotové transakce zpracovávané produktem IBM MQ.
- Detekuje a odebírá zbloudilý nebo neautorizované zprávy před tím, než je zpracován přijímající aplikací.
- Ověřuje, zda během přenosu z fronty do fronty nebyly zprávy změněny.
- Chrání data nejen tak, že teče po síti, ale také při jejich vložení do fronty.
- Zabezpečuje existující vlastní aplikace a aplikace vytvořené zákazníkem pro IBM MQ.
- z/OS V 9.2.0 Z produktu IBM MQ 9.1.3poskytuje produkt IBM MQ for z/OS možnost volitelně odebrat a přidat ochranu AMS z nebo do zpráv, které procházejí přes síť, resp. Tento údaj je známý 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 4se přidá kontrola do kódu knihovny produktu IBM MQ , který je spuštěn v rámci aplikačního programu zákazníka. Kontrola je spuštěna na začátku inicializace a přečetla hodnotu proměnné prostředí *AMQ_AMS_FIPS_OFF* a v případě, že je nastavena na libovolnou hodnotu, je kód sady GSKit spuštěn v režimu non-FIPS v této aplikaci.

Kvality ochrany dostupné s AMS

Pro produkty Advanced Message Security, `Integrity`, `Privacy`a `Confidentiality`jsou k dispozici tři úrovně ochrany.

Ochrana `Integrity` je poskytována digitálním podpisem, který poskytuje ujištění o tom, kdo zprávu vytvořil, a že zpráva nebyla změněna ani upravena.

Ochrana `Privacy` je poskytována kombinací digitálního podepisování a šifrování. Šifrování zajišťuje, že data zprávy lze zobrazit pouze zamýšlenému příjemci nebo příjemcům. I když neautorizovaní příjemci obdrží kopii dat šifrovaných zpráv, nejsou schopni zobrazit samotná data zprávy.

Ochrana `Confidentiality` je poskytována šifrováním pouze s volitelným opětovným použitím klíče.

Vliv na výkon

Produkt AMS používá kombinaci symetrických a asymetrických šifrovacích rutin k poskytování digitálního podepisování a šifrování. Vzhledem k tomu, že symetrické klíčové operace jsou velmi rychle ve srovnání s asymetrickými klíčovými operacemi, které jsou náročné na procesor, může mít tato akce významný dopad na náklady na ochranu velkého počtu zpráv pomocí produktu AMS.

Asymetrické šifrovací rutiny
Například při vložení podepsané zprávy je hašovací funkce zprávy podepsána pomocí asymetrické operace klíče.

Při získávání podepsané zprávy se používá další asymetrická klíčová operace k ověření podepsané hašování.

Proto je požadováno minimálně dva asymetrické klíčové operace na zprávu, abyste mohli podepsat a ověřit data zprávy.

Asymetrické a symetrické kryptografické rutiny
Při vkládání šifrované zprávy je vygenerován symetrický klíč a potom šifrován pomocí asymetrické operace klíče pro každého zamýšleného příjemce zprávy.

Data zprávy jsou poté zašifrována pomocí symetrického klíče. Při získávání šifrované zprávy musí zamýšlený příjemce použít asymetrickou operaci klíče ke zjištění symetrického klíče, který má být použit pro danou zprávu.

Všechny tři úrovně ochrany proto obsahují různé prvky asymetrických klíčových operací náročných na CPU, které významně ovlivní maximální dosažitelnou rychlost systému zpráv pro aplikace umísťujících a získaní zprávy.

`Confidentiality` zásady však umožňují opětovné použití symetrického klíče v posloupnosti zpráv. Výrazné úspory nákladů na jednotku CPU lze provádět pomocí zásad produktu `Confidentiality` prostřednictvím opětovného použití symetrického klíče. Tento provozní režim i nadále používá formát PKCS#7 ke sdílení symetrického šifrovacího klíče. Neexistuje však žádný digitální podpis, který eliminuje některé z operací asymetrického klíče zpráv. Symetrický klíč je stále třeba šifrovat s asymetrickými klíčovými operacemi pro každého příjemce, ale symetrický klíč může být volitelně znovu použit přes více zpráv, které jsou určeny pro stejné příjemce. Je-li opětovné použití klíče povoleno zásadou, pak pouze první zpráva vyžaduje asymetrické operace klíče. Následné zprávy potřebují pouze operace symetrického klíče.

Opětovné použití klíče

Pomocí zásad produktu `Confidentiality` můžete použít přístup pro opětovné použití symetrického klíče k výraznému snížení nákladů spojených s šifrováním určitého počtu zpráv, které jsou vloženy do stejné fronty a určené pro stejného příjemce nebo příjemce.

Například při vložení 10 šifrovaných zpráv do stejné sady příjemců je generován symetrický klíč a pak šifrován pro první zprávu s použitím asymetrické operace klíče pro každého zamýšleného příjemce zprávy.

Na základě omezení řízených zásadami lze zašifrovaný symetrický klíč znovu použít následnými zprávami, které jsou určeny pro stejné příjemce. Chcete-li, aby byl symetrický klíč znovu použit pro následné zprávy, musí aplikace ponechat frontu otevřenou po vložení zprávy do fronty. Symetrický klíč nemohou být znovu použity operacemi MQPUT1 . Aplikace, která získává zašifrované zprávy, může použít stejnou optimalizaci, v tom může aplikace zjistit, kdy se symetrický klíč nezměnil, a vyhnout se nákladům na načtení symetrického klíče.

V tomto příkladu lze vyhnout se 90% asymetrických klíčových operací tím, že se aplikace i získávání aplikací znovu použijí při opětovném použití stejného klíče.

Další informace o tom, jak používat opětovné použití klíče, naleznete v následujících tématech:

- Příkaz MQSC SET POLICY
- Řídicí příkaz setmqspl
- IBM i Příkaz IBM i SETMQMSPL

Klíčové koncepty v produktu AMS

Seznamte se s klíčovými koncepty v produktu Advanced Message Security , abyste porozuměli tomu, jak nástroj funguje a jak efektivně spravovat.

Infrastruktura veřejného klíče a Advanced Message Security

PKI (Public Key Infrastructure) je systém zařízení, zásad a služeb, které podporují použití šifrování pomocí veřejného klíče k získání zabezpečené komunikace.

Neexistuje jediný standard, který definuje komponenty infrastruktury veřejného klíče, ale PKI obvykle zahrnuje použití certifikátů veřejných klíčů a skládá se z certifikačních autorit (CA) a dalších registračních autorit (RA), které poskytují následující služby:

- Vydávání digitálních certifikátů
- Ověření digitálních certifikátů
- Zrušení platnosti digitálních certifikátů
- Distribuce certifikátů

Identita uživatelů a aplikací je reprezentována polem **distinguished name (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 představován popiskem v úložišti klíčů.

Související pojmy

“Použití úložišť klíčů a certifikátů s produktem AMS” na stránce 624
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 produktu AMS

Produkt Advanced Message Security přidružuje uživatele a aplikace k 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 proti ztělesnění tím, že jsou svázáním veřejného klíče jejím vlastníkem, ať už je vlastníkem jednotlivec, správce front nebo jiná entita. Digitální certifikáty jsou také známé jako certifikáty veřejných klíčů, protože poskytují záruku o vlastnictví veřejného klíče, používáte-li asymetrický klíčový plán. Tento program vyžaduje, aby byl pro aplikaci vygenerován veřejný klíč a soukromý klíč. Data zašifrovaná pomocí veřejného klíče lze dešifrovat pouze pomocí odpovídajícího soukromého klíče, zatímco data zašifrovaná pomocí soukromého klíče mohou být dešifrována 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, který se používá k dešifrování zpráv, které jsou šifrovány pomocí odpovídajícího veřejného klíče.

Pokud jsou veřejné klíče odeslány přímo jejich vlastníkem do jiné entity, je zde riziko, že zpráva bude zachycena a veřejný klíč nahradí jiným. To je známo jako útok "man-in-the-middle". Řešením je vyměnit veřejné klíče prostřednictvím důvěryhodné třetí strany a poskytnout uživateli silné ujištění, že veřejný klíč patří k entitě, s níž komunikujete. Namísto přímého odeslání svého veřejného klíče je třeba požádat důvěryhodnou třetí stranu, aby ji začlenila do digitálního certifikátu. Důvěryhodný třetí strana, který vydává digitální certifikáty, se nazývá certifikační autorita (CA).

Další informace o digitálních certifikátech najdete v tématu Co je v digitálním certifikátu.

Digitální certifikát obsahuje veřejný klíč pro entitu a uvádí, že veřejný klíč patří do této entity:

- když se jedná o certifikát pro jednotlivou entitu, nazývá se *osobní certifikát* nebo *uživatelský certifikát*.
- Je-li certifikát pro certifikační autoritu, certifikát se nazývá *certifikát CA* nebo *certifikát podepsaného*.

Poznámka: Produkt Advanced Message Security podporuje certifikáty s vlastním podpisem v produktu Java i v nativních aplikacích

Související pojmy

"Šifrování" na stránce 7

Šifrování je proces převedení mezi čitelným textem, který se nazývá *prostý text*, a nečitelným formulářem s názvem *šifrovaný text*.

Multi *Správce oprávnění k objektu a AMS*

Na více platformách je produkt Object Authority Manager (OAM) součástí autorizační služby dodávané s produkty IBM MQ .

Přístup k entitám Advanced Message Security je řízen pomocí skupin uživatelů produktu IBM MQ a OAM. Administrátoři mohou podle potřeby udělovat nebo odvolávat autorizace pomocí rozhraní příkazového řádku. Různé skupiny uživatelů mohou mít různé druhy přístupových oprávnění ke stejným objektům. Jedna skupina může například provádět operace PUT i GET pro určitou frontu, zatímco jiná skupina může být povolena pouze k procházení fronty. Podobně některé skupiny mohou mít k frontě oprávnění GET a PUT, ale nemohou ji měnit ani odstraňovat.

Prostřednictvím OAM můžete řídit:

- Přístup k objektům produktu Advanced Message Security prostřednictvím rozhraní MQI (Message Queue Interface). Když se aplikační program pokusí o přístup k objektům, zkontroluje program OAM, zda má profil uživatele, který vytvořil 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 produktem Advanced Message Security

Produkt Advanced Message Security závisí na několika technologických komponentách, které zajišťují infrastrukturu zabezpečení.

Produkt Advanced Message Security podporuje následující rozhraní API (Application Programming Interface) 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 odpovídající standardu X.509 .

Známá omezení AMS

Existuje celá řada IBM MQ voleb, které buď nejsou podporovány, nebo mají omezení pro Advanced Message Security.

- Následující volby IBM MQ nejsou podporovány nebo mají omezení:

  Publikování/odběr
  Jednou z hlavních výhod modelu systému zpráv publikování/odběru po pevné lince je to, že odesílající a přijímající aplikace nemusí o sobě vědět nic o datech, která mají být odeslána a přijata. Tento přínos je negován pomocí zásad produktu Advanced Message Security , které musí definovat určené příjemce nebo autorizované podepisující subjekty. Je možné, aby aplikace publikoval do tématu prostřednictvím definice alias fronty, která je chráněna zásadou, je také možné, aby odebírající aplikace získaní zprávy z fronty chráněné zásadami. Není možné přiřadit zásadu přímo k řetězci tématu, zásady lze přiřadit pouze k definicím fronty.

Převod dat kanálu
Chráněný informační obsah chráněné zprávy Advanced Message Security se přenáší pomocí binárního formátu, což zajišťuje, že převod dat na kanálu mezi aplikacemi nezruší platnost kódu digest zprávy. Aplikace, které načítají zprávy z fronty chráněné zásadami, by měly požadovat konverzi dat, po úspěšném ověření a nechránění zpráv se bude pokus o konverzi chráněného informačního obsahu pokoušet.

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 zjištěny nekonzistentní zásady, dojde k selhání operace otevření a k vrácení chyby zabezpečení aplikace.

Segmentace zpráv aplikace
Velikost zpráv chráněných proti zásadám se zvýší a není možné, aby aplikace přesně uváděli hranice segmentu zprávy.

Aplikace využívající produkt IBM MQ classes for .NET ve spravovaném režimu (připojení klienta)
Aplikace, které používají produkt IBM MQ classes for .NET ve spravovaném režimu (připojení klienta), nejsou podporovány.

Poznámka: K povolení nepodporovaných klientů pro použití produktu AMSlze použít zachycení MCA.

Klient služby Message Service pro aplikace produktu .NET (XMS) ve spravovaném režimu
Aplikace klienta Message Service pro aplikace produktu .NET (XMS) ve spravovaném režimu nejsou podporovány.

Poznámka: Interception MCA lze použít k povolení nepodporovaných klientů k použití serveru AMS.

Fronty produktu IBM MQ zpracovávané mostem IMS
Fronty produktu IBM MQ zpracovávané mostu produktu IMS nejsou podporovány.

Poznámka: Produkt AMS je podporován ve frontách mostu CICS . Měli byste použít stejné ID uživatele pro MQPUT (šifrovat) a MQGET (dešifrovat) ve frontách mostu CICS .

Umístit na čekající metodu getter
Vložení k čekající metodě getter není podporováno pro metody getter pro fronty, pro které jsou definovány zásady produktu AMS .

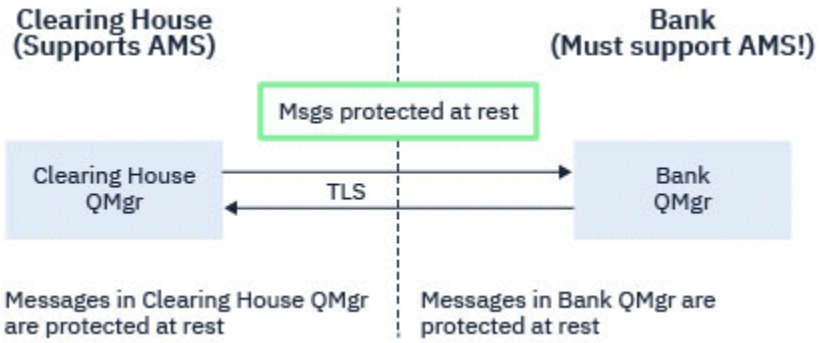
V 9.2.0 **Prokládání serveru MCA pro server**
V produktu IBM MQ for z/OS 9.1.3je server MCA interception serveru podporován pouze pro kanály odesílatele, serveru, příjemce a žadatele.

- Uživatelé by se měli vyhnout vložení více než jednoho certifikátu se stejným rozlišujícím názvem do jednoho souboru úložiště klíčů, protože volba certifikátu, který má být použit při ochraně zprávy, není definován.
- Produkt AMS není podporován v produktu JMS , pokud je vlastnost **WMQ_PROVIDER_VERSION** nastavena na hodnotu 6.
- Zachytávač AMS není podporován pro kanály AMQP nebo MQTT.

z/OS V 9.2.0 Advanced Message Security zachycení na kanálech zpráv

V z/OS, Advanced Message Security (AMS) interception poskytuje další volbu ochrany zásad zabezpečení (SPLPROT) pro kanály odesílatele, serveru, příjemce a žadatele, což vám umožňuje podporovat produkt AMS a komunikovat s obchodními partnery, kteří nepodporují AMS.

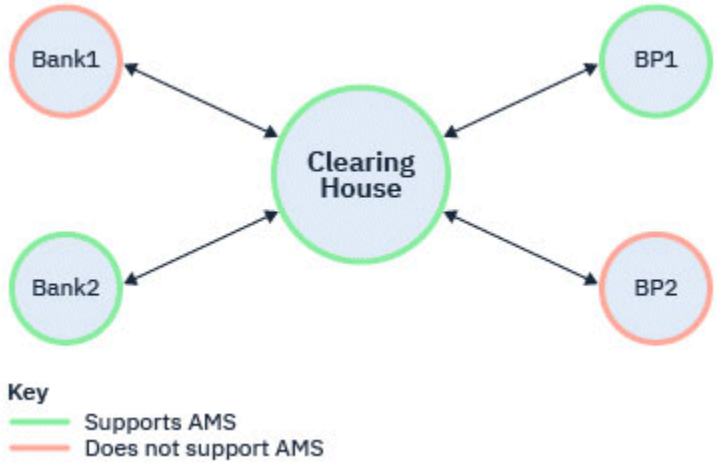
Na příkladu zúčtovacího domu komunikujícího s bankou ukazuje Obrázek 1 , že bez odposlechu AMS musí obě strany systému podporovat AMS.



Obrázek 32. Použití AMS bez odpojičování AMS

Hlavní výhodou možnosti zachycení AMS je, že pokud váš podnik AMS zkonfiguroval, a ne všechny vaše obchodní partnery podporují AMS, můžete odebrat ochranu před odchozími zprávami a chránit příchozí zprávy na kanálech a od těch obchodních partnerů, které nepodporují AMS.

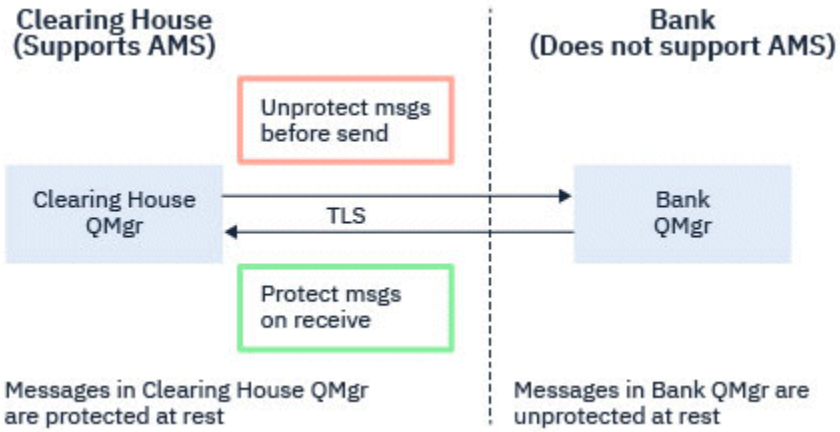
Při použití příkladu clearingového systému a bank se tento scénář zobrazí na Obrázku 2, kde je tok zpráv mezi clearingem, bankami a obchodními partnery, kde některé instituce mají AMSa jiné nikoli.



Obrázek 33. Někteří partneři podporují AMS a některé ne

Typicky jsou kanály TLS povoleny.

Může však nastat situace, kdy některé banky a obchodní partneři nepodporují produkt AMSa je zde požadavek na výměnu zpráv mezi všemi bankami a obchodními partnery. Tento scénář je zobrazen na obrázku 3



Obrázek 34. Tok zpráv mezi obchodními partnery

Související úlohy

Příklady konfigurací serveru zpráv typu server-na-server-zachycení

z/OS V 9.2.0 *Zachycení AMS na kanálech zpráv server-server*

Pokládání zpráv mezi servery poskytuje prostředky k řízení, zda by měly zprávy měly mít všechny použitelné zásady produktu Advanced Message Security (AMS), pokud agenti kanálu zpráv typu odesílatele získají zprávy z přenosových front, a agenti kanálu zpráv typu příjemce vloží zprávy do cílových front.

To umožňuje povolení ochrany produktu AMS ve správci front při komunikaci s kanály zpráv typu odesilatel, server, příjemce a žadatel serveru se správcem front, které nemají povolený produkt AMS .

To znamená, že AMS chráněné zprávy v aktivovaných správci front produktu AMS mohou být nechráněny před tím, než jsou odesílány do správců front s podporou produktuAMS , a nechráněné zprávy přijaté od správců front, kteří nejsou typuAMS , mohou být chráněni příslušnými zásadami produktu AMS v povolených AMS správců front.

Konfigurování zachycení zprávy kanálu na serveru

Pokládání zpráv mezi serverem a serverem je konfigurováno s atributem SPLPROT u kanálů s typem kanálu odesílatele, serveru, přijímače nebo žadatele. 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 zprávy kanálu

Požadavek na ID uživatele používaný při zachycení kanálu zpráv mezi serverem a serverem je stejný jako u existujících aplikací s povoleným produktem AMS . U spuštěného kanálu se odesílající agent kanálu zpráv dostane zprávy z přenosové fronty a přijímající agent kanálu zpráv vloží zprávy do cílových front. Pole ID uživatele agenta kanálu zpráv (MCAUSER), nastavené na serveru pro kanály serveru, definuje ID uživatele, pod kterým agenti kanálu zpráv provádějí operace put a get.

Při zachytávání kanálu zpráv mezi servery se funkce produktu AMS provádějí při získávání a vkládání požadavků stejně jako u jiných aplikací s povoleným produktem AMS . Proto mají ID uživatelů agenta kanálu zpráv stejné požadavky jako ta, která se vztahují k ID uživatelů aplikací produktu AMS .

MCAUSER použitý k provedení vložení a získání je konfigurovatelný a závislý na tom, zda se jedná o odchozí nebo příchozí kanál. Podrobnosti o tom, jak vybrané ID uživatele provádí akce na agentovi oznamovacího kanálu, najdete v části MCAUSER . Jako takové je ID uživatele, pod kterým je spuštěn

inicializátor kanálu, ID uživatele, které má být použito pro funkce produktu AMS prováděné během zachytávání kanálu zpráv serveru na server. Proto mají tato ID uživatele stejné požadavky jako ty, které se vztahují k ID uživatelů aplikací produktu AMS .

Ověřování je prováděno s použitím existujících pravidel pro kanál s podrobnými informacemi o kanálech s konfigurací PUTAUT. Další informace naleznete v tématu ID uživatelů použitá inicializačním programem kanálu .

Poznámka: Při zachycení datového kanálu na serveru k serveru se nebere v úvahu hodnota atributu PUTAUT kanálu.

Velikost zprávy a MAXMSGL

Kvůli ochraně produktu AMS bude velikost zpráv chráněných zpráv větší než původní velikost zprávy.

Chráněné zprávy jsou větší než nezabezpečené zprávy. Proto může být nutné změnit hodnotu atributu **MAXMSGL** u obou front a kanálů, aby bylo možné zohlednit velikost chráněných zpráv.

Související odkazy

Příklady konfigurací serveru zpráv typu server-na-server-zachycení

Ošetření chyb pro AMS

IBM MQ Advanced Message Security definuje frontu zpracování chyb pro správu zpráv, které obsahují chyby nebo zprávy, které nemohou být nechráněné.

Vadné zprávy se řeší jako výjimečné případy. Pokud přijatá zpráva nesplňuje požadavky na zabezpečení fronty, například pokud je zpráva podepsána, když by měla být šifrována, nebo selže dešifrování nebo ověření podpisu, zpráva se odešle do fronty zpracování chyb. Zpráva může být odeslána do fronty zpracování chyb z následujících důvodů:

- Neshoda kvality ochrany-mezi přijatou zprávou a definicí QOP v rámci zásady zabezpečení existuje neshoda kvality ochrany (QOP).
- Chyba dešifrování-zpráva nemůže být dešifrována.
- Chyba záhlaví PDMQ-nelze získat přístup k záhlaví zprávy produktu Advanced Message Security (AMS).
- Nesrovnalost velikosti-délka zprávy po dešifrování je jiná, než se očekávalo.
- Neshoda odolnosti algoritmu šifrování-algoritmus šifrování zpráv je slabší, než je požadováno.
- Neznámá chyba-došlo k neočekávané chybě.

Produkt AMS používá SYSTEM.PROTECTION.ERROR.QUEUE jako frontu zpracování chyb. Všechny zprávy odeslané produktem IBM MQ AMS do systému SYSTEM.PROTECTION.ERROR.QUEUE je předcházena hlavičkou MQDLH.

Administrátor produktu IBM MQ může také definovat SYSTEM.PROTECTION.ERROR.QUEUE jako fronta aliasů odkazující na jinou frontu.

z/OS V 9.2.0 From IBM MQ 9.1.3, on IBM MQ for z/OS, if server to server Message Channel Agent (MCA) interception is in use:

- Pokud kvůli jednomu z výše uvedených důvodů produkt IBM MQ AMS přesouvá zprávy z přenosové fronty do fronty pro zpracování chyb, agent MCA jednoduše pokračuje zpracováním další dostupné zprávy v přenosové frontě.
- Obecně platí, že se použijí existující pravidla kanálu pro:
  - Vložení zpráv do fronty nedoručených zpráv a
  - Akce, které se provedou při vložení do fronty nedoručených zpráv, by měly selhat.

Další informace o specifických scénářích naleznete v tématu “Nedoručené zprávy pro AMS v systému z/OS” na stránce 589 .

z/OS V 9.2.0 *Nedoručené zprávy pro AMS v systému z/OS*

Specifické scénáře vztahující se k serveru na zachycení agenta Message Channel Agent na serveru IBM MQ for z/OS.

From IBM MQ 9.1.3, on IBM MQ for z/OS, if server to server Message Channel Agent (MCA) interception is in use:

- Pokud má odesilatel MCA po získání a nechráněné zprávě doručit zprávu z nějakého důvodu, například protože je zpráva pro kanál příliš velká, pokud je atribut kanálu odesílatele USEDLQ nastaven na hodnotu YES, přesune odesilatel MCA zprávu do lokální fronty nedoručených zpráv (DLQ).

  Pokud je SYSTEM.DEAD.LETTER.QUEUE se používá jako lokální DLQ, zpráva je nechráněná.

  Poznámka: Produkt IBM MQ AMS nepodporuje ochranu zpráv vložených do systémových front.

  Je-li jako lokální DLQ použita pojmenovaná fronta nedoručených zpráv, bude tato zpráva chráněna, pokud jste definovali zásadu IBM MQ AMS se stejným názvem jako název fronty DLQ a nechráněná, pokud jste nedefinovali vhodnou zásadu.
- Pokud zprávu z nějakého důvodu nelze vložit do lokálního DLQ, pak je-li NPMSPEED kanálu nastaveno na NORMAL nebo se jedná o trvalou zprávu, aktuální dávka zpráv se zálohována a kanál vložen do stavu RETRY. Jinak bude zpráva vyřazena a odesilatel MCA pokračuje ve zpracování další zprávy v přenosové frontě.
- Vzhledem k tomu, že zásady zabezpečení nemají žádný vliv na SYSTEM.DEAD.LETTER.QUEUEnebo jiné fronty SYSTEM uvedené v části “Ochrana systémových front v produktu AMS” na stránce 659, pokud je SYSTEM.DEAD.LETTER.QUEUE je používána, zprávy vložené do této fronty pomocí MCA jsou umístěny tak, jak jsou. To znamená, že pokud byly zprávy dříve chráněné, jsou umístěny pod ochranou; v opačném případě jsou umístěny nechráněné.

  Pokud byl atribut DEADQ správce front nastaven na název alternativní fronty nedoručených zpráv (ne systém) a zásada AMS se stejným názvem neexistuje, budou zprávy vložené do této fronty serverem MCA umístěny tak, jak jsou. To znamená, že pokud byly zprávy dříve chráněné, jsou umístěny pod ochranou; v opačném případě jsou umístěny nechráněné.

  Pokud byl atribut DEADQ správce front nastaven na název alternativní fronty nedoručených zpráv (jiná než systémová) a zásada AMS se stejným názvem jako má fronta DLQ, zásada se použije k ochraně zpráv vložených do této fronty pomocí rozhraní MCA. Pokud již byla zpráva již dříve chráněna, není znovu chráněna; toto je ochrana proti dvojí ochraně. Pokud zásada AMS se stejným názvem neexistuje, zprávy se umístí tak, jak jsou.
- Existuje-li zásada pro frontu nedoručených zpráv s možností tolerance v příkazu setmqspl , která je nastavena na hodnotu '**-t** O', vložení do fronty DLQ selže, pokud zpráva není chráněna AMS , a proto neobsahuje záhlaví PDMQ. K tomu dojde, pokud zpráva dorazí do přijímače bez záhlaví PDMQ. To znamená, že původní putter zprávy nemá pro cíl zásadu, a příjemce nemá nastaven parametr SPLPROT (ASPOLICY).
- MCA může selhat při vložení zprávy do fronty DLQ, pokud zásada AMS definovaná pro DLQ nepovoluje ID uživatele, pod kterým je spuštěn inicializátor kanálu, aby chránil tuto zprávu.
- Přijímací kanály obvykle umisťují nedoručené zprávy do lokálního DLQ, zatímco odesílací kanály obvykle umisťují zprávy, které nemohou být zpracovány z nějakého důvodu, například zpráva je příliš velká pro frontu nebo špatné záhlaví MQXQH, a tak dále na lokální DLQ.
- Obslužné rutiny DLQ se obvykle podívají pouze na záhlaví DLQ (DLH) a nikoli o samotný informační obsah zprávy. Takže skutečnost, že informační obsah zprávy může být chráněna, nezabrání obslužnými rutinám zjistit, proč byla zpráva umístěna do fronty nedoručených zpráv.
- Není-li fronta DLQ definována, kanál:
  - Ukončuje abnormálně (a přejde do stavu opakování), pokud nelze doručit trvalou zprávu.
  - Vyřadí netrvalou nedoručenou zprávu a pokračuje v jejím spuštění.

Související pojmy

“Ošetření chyb pro AMS” na stránce 588

IBM MQ Advanced Message Security definuje frontu zpracování chyb pro správu zpráv, které obsahují chyby nebo zprávy, které nemohou být nechráněné.

Uživatelské scénáře pro AMS

Seznamte se s možnými scénáři a seznamte se s obchodními cíli, které lze dosáhnout pomocí produktu Advanced Message Security.

Windows *Stručná úvodní příručka pro produkt AMS na platformách Windows*

Pomocí této příručky můžete rychle nakonfigurovat produkt Advanced Message Security tak, aby poskytoval zabezpečení zpráv na platformách Windows . Po dokončení této operace jste vytvořili databázi klíčů k ověření identit uživatelů a definované zásady podepisování a šifrování pro správce front.

Než začnete

V systému by měly být nainstalovány alespoň následující funkce:

- Server
- Development Toolkit (pro vzorové programy)
- Advanced Message Security

Podrobné informace naleznete v tématu Funkce produktuIBM MQ pro systémy Windows .

Informace o použití příkazu **setmqenv** k inicializaci aktuálního prostředí tak, aby příslušné příkazy produktu IBM MQ mohly být umístěny a spuštěny operačním systémem, viz setmqenv (nastavit prostředí IBM MQ).

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 místě, ve kterém vstupují do infrastruktury produktu IBM MQ prostřednictvím standardního rozhraní produktu IBM MQ . Základní nastavení se provádí v produktu IBM MQ a je konfigurováno v následujících krocích.

Pomocí produktu IBM MQ Explorer můžete vytvořit správce front QM_VERIFY_AMS a jeho lokální frontu s názvem `TEST.Q` tak, že použijete všechna výchozí nastavení průvodce, nebo můžete použít příkazy nalezené v `C:\Program Files\IBM\MQ\bin`. Nezapomeňte, že musíte být členem skupiny uživatelů produktu `mqm` , chcete-li 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 produktu **runmqsc** pro správce front `QM_VERIFY_AMS`

   ```
   DEFINE QLOCAL(TEST.Q)
   ```

Výsledky

Je-li procedura dokončena, příkaz zadaný do **runmqsc** zobrazí podrobnosti o TEST.Q:

```
DISPLAY Q(TEST.Q)
```

2. Vytvoření a autorizace uživatelů

Informace o této úloze

V tomto příkladu se objevují dva uživatelé: `alice`, odesílatel a bob, příjemce. K tomu, abyste mohli používat aplikační frontu, je třeba těmto uživatelům udělit oprávnění k jeho používání. Také pro úspěšné použití zásad ochrany, které nadefinujeme těmto uživatelům, musí být udělen přístup k některým systémovým frontám. Další informace o příkazu **setmqaut** naleznete v části **setmqaut**.

Postup

1. Vytvořte dva uživatele a ujistěte se, že jsou pro oba tyto uživatele nastaveny parametry HOMEPATH a HOMEDRIVE .
2. Autorizovat uživatele pro připojení ke správci front a pro práci s touto 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 povolit, aby dva uživatelé procházeli frontu zásad systému a vložili 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 pomocí zásad ukládání do mezipaměti, takže nemusíte procházet záznamy o podrobnostech zásady v systému SYSTEM.PROTECTION.POLICY.QUEUE ve všech případech.

   Produkt IBM MQ neukládá do mezipaměti všechny dostupné zásady. Existuje-li vysoký počet zásad, produkt IBM MQ ukládá omezený počet zásad do mezipaměti. Má-li tedy správce front definován nízký počet definovaných zásad, není třeba zadávat volbu procházení do systému SYSTEM.PROTECTION.POLICY.QUEUE.

   Do této fronty byste však měli udělit oprávnění k procházení, v případě, že je definován vysoký počet zásad, nebo pokud používáte staré klienty. SYSTEM.PROTECTION.ERROR.QUEUE se používá k vložení chybových zpráv generovaných kódem AMS. Oprávnění k vložení pro tuto frontu se kontroluje pouze tehdy, když se pokusíte vložit chybovou zprávu do fronty. Při pokusu o vložení nebo získání zprávy z chráněné fronty AMS se nekontroluje vaše oprávnění k zařazení do fronty.

Výsledky

Uživatelé jsou nyní vytvořni a požadovaná oprávnění jim byla udělena.

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 594.

3. Vytvoření databáze klíčů a certifikátů

Informace o této úloze

Zachytávač vyžaduje veřejný klíč odesílajícího uživatele k zašifrování zprávy. Proto musí být vytvořena klíčová databáze identit uživatelů namapovaných na veřejné a soukromé klíče. V reálném systému, kde uživatelé a aplikace jsou rozptýleni přes několik počítačů, by měl každý uživatel své vlastní soukromé úložiště klíčů. Podobně v této příručce vytváříme databáze klíčů pro `alice` a bob a sdílíme uživatelské certifikáty mezi nimi.

Poznámka: V této příručce používáme vzorové aplikace napsané v C, které se připojují pomocí lokálních vazeb. Plánujete-li používat aplikace produktu Java s použitím vazeb klienta, je nutné vytvořit úložiště klíčů a certifikáty JKS pomocí příkazu **keytool** , který je součástí prostředí JRE (další podrobnosti viz “Stručná úvodní příručka pro AMS s klienty Java” na stránce 612). Kroky v této příručce jsou správné pro všechny ostatní jazyky a pro aplikace Java používající lokální vazby.

Postup

1. Použijte grafické rozhraní Správa klíčů produktu IBM (`strmqikm.exe`) chcete-li vytvořit novou databázi klíčů pro uživatele `alice`.

   ```
   Type:       CMS
   Filename:   alicekey.kdb
   Location:   C:/Documents and Settings/alice/AMS
   ```

   Poznámka:

   - Je vhodné použít silné heslo k zabezpečení databáze.
   - Ujistěte se, že je vybráno zaškrtávací políčko **Stash password to a file** .
2. Změňte zobrazení obsahu databáze klíčů na **Osobní certifikáty**.
3. Vyberte volbu **Nový samopodepsaný** ; v tomto scénáři se používají certifikáty s vlastním podpisem.
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 držitelem, který může být vytvořen bez použití certifikační autority. U výrobních systémů se doporučuje nepoužívat certifikáty podepsané sebou samým, ale spíše spoléhat na certifikáty podepsané vydavatelem certifikátů.
   - Parametr **Key label** určuje název certifikátu, který zachytávače vyhledají, aby obdrželi potřebné informace.
   - Parametry **Common Name** a nepovinné parametry uvádí podrobnosti o **rozlišujícím názvu** (DN), které musí být jedinečné pro každého uživatele.
5. Opakovat krok 1-4 pro uživatele bob

Výsledky

Dva uživatelé `alice` a bob mají každý nyní certifikát podepsaný svým držitelem.

4. Vytvoření souboru keystore.conf

Informace o této úloze

Do adresáře, kde jsou umístěny databáze klíčů a certifikáty, musíte zabodávat zachytávače Advanced Message Security . To se provádí prostřednictvím souboru `keystore.conf` , který obsahuje informace

v podobě prostého textu. Každý uživatel musí mít samostatný soubor `keystore.conf` ve složce `.mqs` . Tento krok musí být proveden jak pro `alice` , tak pro bob.

Obsah produktu `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.
- Návěští certifikátu může obsahovat mezery, tedy "Alice_Cert" a "Alice_Cert" (s prostorem na konci) například jsou rozpoznány jako popisky dvou různých certifikátů. Aby se však předešlo nejasnostem, je lepší nepoužívat mezery v názvu návěští.
- K dispozici jsou následující formáty úložiště klíčů: CMS (Syntaxe kryptografických zpráv), JKS (Java Úložiště klíčů) a JCEKS (Java Cryptographic Extension Keystore). Další informace jsou uvedeny v tématu “Struktura konfiguračního souboru úložiště klíčů (keystore.conf) pro AMS” na stránce 625.
- *%HOMEDRIVE%\%HOMEPATH%*\`.mqs\keystore.conf` (např. C:\Documents and Settings\alice\.mqs\keystore.conf) je výchozí umístění, kde Advanced Message Security hledá soubor `keystore.conf` . Informace o tom, jak používat jiné než výchozí umístění pro produkt `keystore.conf`, viz “Použití úložišť klíčů a certifikátů s produktem AMS” na stránce 624.
- Chcete-li vytvořit adresář `.mqs` , musíte použít příkazový řádek.

5. Sdílení certifikátů

Informace o této úloze

Sdílejte certifikáty mezi dvěma klíčovými databázemi tak, aby každý uživatel mohl úspěšně identifikovat ostatní. To se provádí extrahováním veřejného certifikátu každého uživatele do souboru, který je poté přidán do databáze klíčů druhého uživatele.

Poznámka: Dávejte pozor, abyste použili volbu *extract* , a ne volbu *export* . Volba *Extrahovat* získá veřejný klíč uživatele, zatímco *export* získá veřejný i soukromý klíč. Použití *exportu* omylem by zcela ohrozilo vaši aplikaci tím, že se předá na soukromý klíč.

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 produktu `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 navzájem úspěšně identifikovat, protože vytvořili a sdíleli certifikáty podepsané sebou samým.

Jak pokračovat dále

Ověřte, že je certifikát v úložišti klíčů buď tím, že jej prohledáváním 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

Se správcem front vytvořeným a zachytávačem připraveným k zachycení zpráv a přístupu k šifrovacím klíčům můžeme začít definovat zásady ochrany na systému `QM_VERIFY_AMS` pomocí příkazu `setmqspl` . Další informace o tomto příkazu najdete v souboru setmqspl . Každý název zásady musí být stejný jako název fronty, na který se má použít.

Příklad

Toto je příklad zásady definované pro frontu `TEST.Q` . V tomto příkladu jsou zprávy podepsány s algoritmem SHA1 a šifrovány pomocí algoritmu AES256 . `alice` je jediný platný odesílatel 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 certifikátu příslušného uživatele od 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 parametr `-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 řádně nakonfigurována.

Postup

1. Přepnout uživatele ke spuštění jako uživatel `alice`

   Klepněte pravým tlačítkem myši na `cmd.exe` a vyberte **Spustit jako ...**. Jste-li vyzváni, přihlaste se jako uživatel `alice`.
2. Protože uživatel `alice` vložil zprávu pomocí ukázkové aplikace, postupujte takto:

   ```
   amqsput TEST.Q QM_VERIFY_AMS
   ```
3. Zadejte text zprávy a pak stiskněte klávesu Enter.
4. Přepnout uživatele ke spuštění jako uživatel bob

   Otevřete další okno tak, že klepnete pravým tlačítkem myši na `cmd.exe` a vyberete **Spustit jako ...**. Jste-li vyzváni, přihlaste se jako uživatel bob.
5. Když uživatel bob získá zprávu pomocí ukázkové aplikace, postupujte takto:

   ```
   amqsget TEST.Q QM_VERIFY_AMS
   ```

Výsledky

Pokud byla aplikace správně nakonfigurována pro oba uživatele, zobrazí se zpráva uživatele `alice` , když produkt bob spustí aplikaci získání.

8. Testování šifrování

Informace o této úloze

Chcete-li ověřit, zda se šifrování provádí 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 se budou zobrazovat šifrovaná data.

Postup

1. Pomocí příkazu **`runmqsc`** pro správce front QM_VERIFY_AMS vytvořte alias frontu.

   ```
   DEFINE QALIAS(TEST.ALIAS) TARGET(TEST.Q)
   ```
2. Udělte uživateli bob přístup k procházení z fronty aliasů

   ```
   setmqaut -m QM_VERIFY_AMS -n TEST.ALIAS -t queue -p bob +browse
   ```
3. Jako uživatel `alice`vložte jinou zprávu pomocí ukázkové aplikace stejně jako předtím:

   ```
   amqsput TEST.Q QM_VERIFY_AMS
   ```
4. Jako uživatel bobprocházejte zprávou s použitím ukázkové aplikace přes alias fronty tentokrát:

   ```
   amqsbcg TEST.ALIAS QM_VERIFY_AMS
   ```
5. Jako uživatel bobzískejte zprávu s použitím ukázkové aplikace z lokální fronty:

   ```
   amqsget TEST.Q QM_VERIFY_AMS
   ```

Výsledky

Výstup z aplikace `amqsbcg` zobrazuje šifrovaná data, která jsou ve frontě potvrzující, že zpráva byla šifrována.

Linux AIX *Stručná úvodní příručka pro AMS v systému AIX and Linux*

Pomocí této příručky můžete rychle nakonfigurovat produkt Advanced Message Security tak, aby poskytoval zabezpečení zpráv produktu AIX and Linux. Po dokončení této operace jste vytvořili databázi klíčů k ověření identit uživatelů a definované zásady podepisování a šifrování pro správce front.

Než začnete

V systému by měly být nainstalovány alespoň následující komponenty:

- Běhové prostředí
- Server
- Ukázkové programy.
- IBM Sada globálního zabezpečení
- Advanced Message Security

Názvy komponent na každé specifické platformě naleznete v následujících tématech:

- Linux Komponenty produktuIBM MQ pro systémy Linux
- AIX Komponenty produktuIBM MQ pro systémy AIX

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 místě, ve kterém vstupují do infrastruktury produktu IBM MQ prostřednictvím standardního rozhraní produktu IBM MQ . Základní nastavení se provádí v produktu IBM MQ a je konfigurováno v následujících krocích.

Pomocí produktu IBM MQ Explorer můžete vytvořit správce front QM_VERIFY_AMS a jeho lokální frontu s názvem TEST.Q tak, že použijete všechna výchozí nastavení průvodce, nebo můžete použít příkazy nalezené v *MQ_INSTALLATION_PATH*/bin. Nezapomeňte, že musíte být členem skupiny uživatelů produktu mqm , chcete-li 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 produktu **runmqsc** pro správce front QM_VERIFY_AMS

   ```
   DEFINE QLOCAL(TEST.Q)
   ```

Výsledky

Pokud byla procedura úspěšně dokončena, zobrazí se následující příkaz zadaný do **runmqsc** zobrazí podrobnosti o TEST.Q:

```
DISPLAY Q(TEST.Q)
```

2. Vytvoření a autorizace uživatelů

Informace o této úloze

V tomto příkladu se objevují dva uživatelé: `alice`, odesílatel a `bob`, příjemce. K tomu, abyste mohli používat aplikační frontu, je třeba těmto uživatelům udělit oprávnění k jeho používání. Také pro úspěšné použití zásad ochrany, které nadefinujeme těmto uživatelům, musí být udělen přístup k některým systémovým frontám. Další informace o příkazu **setmqaut** naleznete v části **setmqaut**.

Postup

1. Vytvoření dvou uživatelů

```
useradd alice
useradd bob
```

2. Autorizovat uživatele pro připojení ke správci front a pro práci s touto 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 povolit, aby dva uživatelé procházeli frontu zásad systému a vložili 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 pomocí zásad ukládání do mezipaměti, takže nemusíte procházet záznamy o podrobnostech zásady v systému SYSTEM.PROTECTION.POLICY.QUEUE ve všech případech.

Produkt IBM MQ neukládá do mezipaměti všechny dostupné zásady. Existuje-li vysoký počet zásad, produkt IBM MQ ukládá omezený počet zásad do mezipaměti. Má-li tedy správce front definován nízký počet definovaných zásad, není třeba zadávat volbu procházení do systému SYSTEM.PROTECTION.POLICY.QUEUE.

Do této fronty byste však měli udělit oprávnění k procházení, v případě, že je definován vysoký počet zásad, nebo pokud používáte staré klienty. SYSTEM.PROTECTION.ERROR.QUEUE se používá k vložení chybových zpráv generovaných kódem AMS. Oprávnění k vložení pro tuto frontu se kontroluje pouze tehdy, když se pokusíte vložit chybovou zprávu do fronty. Při pokusu o vložení nebo získání zprávy z chráněné fronty AMS se nekontroluje vaše oprávnění k zařazení do fronty.

Výsledky

Uživatelské skupiny jsou nyní vytvořeny a požadovaná oprávnění jim byla udělena. Uživatelé, kteří jsou přiřazeni těmto skupinám, budou mít také oprávnění k připojení ke správci front a k 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 601.

3. Vytvoření databáze klíčů a certifikátů

Informace o této úloze

Pro zašifrování zprávy zachytávač vyžaduje soukromý klíč odesílajícího uživatele a veřejný klíč (y) příjemce (ů). Proto musí být vytvořena klíčová databáze identit uživatelů namapovaných na veřejné a soukromé

klíče. V reálném systému, kde uživatelé a aplikace jsou rozptýleni přes několik počítačů, by měl každý uživatel své vlastní soukromé úložiště klíčů. Podobně v této příručce vytváříme databáze klíčů pro `alice` a bob a sdílíme uživatelské certifikáty mezi nimi.

Poznámka: V této příručce používáme vzorové aplikace napsané v C, které se připojují pomocí lokálních vazeb. Plánujete-li používat aplikace produktu Java s použitím vazeb klienta, je nutné vytvořit úložiště klíčů a certifikáty JKS pomocí příkazu **keytool** , který je součástí prostředí JRE (další podrobnosti viz “Stručná úvodní příručka pro AMS s klienty Java” na stránce 612). Kroky v této příručce jsou správné pro všechny ostatní jazyky a pro aplikace Java používající lokální vazby.

Postup

1. Vytvoření nové databáze klíčů pro uživatele `alice`

   ```
   mkdir /home/alice/.mqs -p
   runmqakm -keydb -create -db /home/alice/.mqs/alicekey.kdb -pw passw0rd -stash
   ```

   Poznámka:

   - Je vhodné použít silné heslo k zabezpečení databáze.
   - 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. Vytvořit 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 držitelem, který může být vytvořen bez použití certifikační autority. U výrobních systémů se doporučuje nepoužívat certifikáty podepsané sebou samým, ale spíše spoléhat na certifikáty podepsané vydavatelem certifikátů.
   - Parametr **label** určuje název certifikátu, který zachytávače vyhledají, aby obdrželi potřebné informace.
   - Parametr **DN** určuje podrobnosti o **rozlišujícím názvu** (DN), které musí být jedinečné pro každého uživatele.
4. Nyní jsme vytvořili databázi klíčů, měli bychom nastavit její vlastnictví a zajistit, aby ji nečitelná všichni ostatní uživatelé.

   ```
   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. Opakovat krok 1-4 pro uživatele bob

Výsledky

Dva uživatelé `alice` a bob mají každý nyní certifikát podepsaný svým držitelem.

4. Vytvoření souboru keystore.conf

Informace o této úloze

Do adresáře, kde jsou umístěny databáze klíčů a certifikáty, musíte zabodávat zachytávače Advanced Message Security . To se provádí prostřednictvím souboru `keystore.conf` , který obsahuje informace

v podobě prostého textu. Každý uživatel musí mít samostatný soubor `keystore.conf` ve složce `.mqs` . Tento krok musí být proveden jak pro `alice` , tak pro bob.

Obsah produktu `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.
- K dispozici jsou následující formáty úložiště klíčů: CMS (Syntaxe kryptografických zpráv), JKS (Java Úložiště klíčů) a JCEKS (Java Cryptographic Extension Keystore). Další informace jsou uvedeny v tématu “Struktura konfiguračního souboru úložiště klíčů (keystore.conf) pro AMS” na stránce 625.
- `HOME/.mqs/keystore.conf` je výchozí umístění, kde Advanced Message Security hledá soubor `keystore.conf` . Informace o tom, jak používat jiné než výchozí umístění pro produkt `keystore.conf`, viz “Použití úložišť klíčů a certifikátů s produktem AMS” na stránce 624.

5. Sdílení certifikátů

Informace o této úloze

Sdílejte certifikáty mezi dvěma klíčovými databázemi tak, aby každý uživatel mohl úspěšně identifikovat ostatní. To se provádí extrahováním veřejného certifikátu každého uživatele do souboru, který je poté přidán do databáze klíčů druhého uživatele.

Poznámka: Dávejte pozor, abyste použili volbu *extract* , a ne volbu *export* . Volba *Extrahovat* získá veřejný klíč uživatele, zatímco *export* získá veřejný i soukromý klíč. Použití *exportu* omylem by zcela ohrozilo vaši aplikaci tím, že se předá na soukromý klíč.

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 produktu `bob's` :

   ```
   runmqakm -cert -add -db /home/bob/.mqs/bobkey.kdb -pw passw0rd -label Alice_Cert -file
   alice_public.arm
   ```

3. Zopakujte tento krok pro bob:

   ```
   runmqakm -cert -extract -db /home/bob/.mqs/bobkey.kdb -pw passw0rd -label Bob_Cert -target
   bob_public.arm
   ```

4. Add the certificate for bob to `alice's` keystore:

   ```
   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 navzájem úspěšně identifikovat, protože vytvořili a sdíleli certifikáty podepsané sebou samým.

Jak pokračovat dále

Spuštěním následujících příkazů, které vytisknou jeho podrobnosti, ověřte, že je certifikát v úložišti klíčů:

```
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

Se správcem front vytvořeným a zachytávačem připraveným k zachycení zpráv a přístupu k šifrovacím klíčům můžeme začít definovat zásady ochrany na systému `QM_VERIFY_AMS` pomocí příkazu `setmqspl` . Další informace o tomto příkazu najdete v souboru setmqspl . Každý název zásady musí být stejný jako název fronty, na který se má použít.

Příklad

Toto je příklad zásady definované pro frontu `TEST.Q` . V tomto příkladě jsou zprávy podepsány uživatelem `alice` pomocí algoritmu SHA1 a šifrovány pomocí 256bitového algoritmu AES . `alice` je jediný platný odesílatel 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 certifikátu příslušného uživatele od 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 parametr `-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 řádně nakonfigurována.

Postup

1. Přejděte do adresáře obsahujícího ukázky. Je-li produkt MQ nainstalován v jiném než výchozím umístění, může se jednat o jiné místo.

   ```
   cd /opt/mqm/samp/bin
   ```

2. Přepnout uživatele ke spuštění jako uživatel `alice`

```
su alice
```

3. Jako uživatel `alice`vložte zprávu s použitím ukázkové aplikace:

```
./amqsput TEST.Q QM_VERIFY_AMS
```

4. Zadejte text zprávy a pak stiskněte klávesu Enter.
5. Zastavení běhu jako uživatel `alice`

```
exit
```

6. Přepnout uživatele ke spuštění jako uživatel bob

```
su bob
```

7. Jako uživatel bobse zobrazí zpráva s použitím 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 aplikaci získání.

8. Testování šifrování

Informace o této úloze

Chcete-li ověřit, zda se šifrování provádí 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 se budou zobrazovat šifrovaná data.

Postup

1. Pomocí příkazu **runmqsc** pro správce front QM_VERIFY_AMS vytvořte alias frontu.

```
DEFINE QALIAS(TEST.ALIAS) TARGET(TEST.Q)
```

2. Udělte uživateli bob přístup k procházení z fronty aliasů

```
setmqaut -m QM_VERIFY_AMS -n TEST.ALIAS -t queue -p bob +browse
```

3. Jako uživatel `alice`vložte jinou zprávu pomocí ukázkové aplikace stejně jako předtím:

```
./amqsput TEST.Q QM_VERIFY_AMS
```

4. Jako uživatel bobprocházejte zprávou s použitím ukázkové aplikace přes alias fronty tentokrát:

```
./amqsbcg TEST.ALIAS QM_VERIFY_AMS
```

5. Jako uživatel bobzískejte zprávu s použitím ukázkové aplikace z lokální fronty:

```
./amqsget TEST.Q QM_VERIFY_AMS
```

Výsledky

Výstup z aplikace `amqsbcg` bude zobrazovat šifrovaná data, která jsou ve frontě potvrzující, že zpráva byla šifrována.

z/OS *Příklad konfigurace produktu AMS v systému z/OS*

Tato část obsahuje vzorové konfigurace zásad a certifikátů pro Advanced Message Security scénáře řazení do fronty v produktu z/OS.

Podrobnosti o konfiguraci produktu Advanced Message Securityviz Konfigurace prostoru Advanced Message Security for z/OS .

Příklady zahrnují požadované zásady produktu Advanced Message Security a digitální certifikáty, které musí existovat vzhledem k uživatelům a klíčům klíčů. Příklady předpokládají, že uživatelé, kteří se podíleli na scénáři, byli nastavenými podle pokynů uvedených v tématu Udělení oprávnění k prostředkům uživatelům pro produkt Advanced Message Security.

V 9.2.0 Dále dále od IBM MQ 9.1.3 viz příklady zachycení kanálu zpráv mezi serverem.

z/OS *Lokální ukládání zpráv s ochranou integrity do fronty pro produkt AMS v systému z/OS*

Tento příklad podrobně popisuje zásady a certifikáty produktu Advanced Message Security potřebné k odesílání a načítání zpráv chráněných integritou do fronty a z fronty, která je lokální vzhledem k ukládání a získávání aplikací.

Ukázkový správce front a fronta jsou:

```
BNK6        - Queue manager
FIN.XFER.Q7 - Local queue
```

Tito uživatelé se používají:

```
WMQBNK6  - AMS task user
TELLER5  - Sending user
FINADM2  - Recipient user
```

Vytvoření uživatelských certifikátů

V tomto příkladu je potřeba pouze jeden uživatelský certifikát. Jedná se o certifikát pro odeslání uživatele, který je nutný pro podepisování zpráv chráněných integrity. Odesílající uživatel je 'TELLER5'.

Je také požadován certifikát vydavatele certifikátů (CA). Certifikát CA je certifikát autority, která vydala certifikát uživatele. Může se jednat o řetězec certifikátů. Je-li tomu tak, 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 RACDCERT produktu RACF . 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 procedury pro výběr nebo vytvoření certifikátu CA, stejně jako procedury pro vydávání certifikátů a distribuci těchto certifikátů do příslušných systémů.

Při exportu a importu těchto certifikátů produkt Advanced Message Security vyžaduje:

- Certifikát CA (řetězec).
- Certifikát uživatele a jeho soukromý klíč.

Používáte-li produkt RACF, lze příkaz RACDCERT EXPORT použít k exportování certifikátů do datové sady a příkaz RACDCERT ADD lze použít k importování certifikátů z datové sady. Další informace o těchto a jiných příkazech RACDCCERT naleznete v tématu *z/OS: Referenční příručka jazyka příkazů zabezpečení serveru RACF Security Server*.

Certifikáty v tomto případě jsou vyžadovány na systému z/OS se spuštěným správcem front BNK6.

Pokud byly certifikáty importovány do systému z/OS se systémem BNK6, je tento certifikát uživatele vyžadován atributem TRUST. Příkaz RACDRCERT ALTER lze použít k přidání atributu TRUST do certifikátu. Příklad:

```
RACDCERT ID(TELLER5) ALTER (LABEL('Teller5')) TRUST
```

V tomto příkladu není pro uživatele příjemce požadován žádný certifikát.

Připojení certifikátů k příslušným klíčovým sdružením

Pokud byly požadované certifikáty vytvořeny nebo importovány a nastaveny jako důvěryhodné, musí být připojeny k příslušným prstenům klíčů uživatele na systému z/OS , kde je spuštěna 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 odesílající uživatele, 'TELLER5'. Mějte na zřeteli, že název svazku klíčů drq.ams.keyring je povinný a název rozlišuje velká a malá písmena.

Když byly vytvořeny svazky klíčů, mohou být příslušné certifikáty připojeny:

```
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 se certifikát uživatele musí být připojen jako VÝCHOZÍ. Pokud má odesílající uživatel více než jeden certifikát ve svém souboru drq.ams.keyring, použije se výchozí certifikát pro účely podepisování.

Vytvoření a úprava certifikátů nejsou produktem Advanced Message Security rozpoznány, dokud není správce front zastaven a restartován, nebo se příkaz z/OS **MODIFY** používá k aktualizaci konfigurace certifikátu produktu Advanced Message Security . Příklad:

```
F BNK6AMSM,REFRESH KEYRING
```

Vytvoření zásady produktu Advanced Message Security

V tomto příkladu jsou zprávy chráněné integrity vloženy do fronty FIN.XFER.Q7 z aplikace spuštěné jako uživatel 'TELLER5' a načtené ze stejné fronty aplikací spuštěnými jako uživatel 'FINADM2', takže je vyžadována pouze jedna zásada Advanced Message Security .

Zásady produktu Advanced Message Security se vytvářejí pomocí obslužného programu CSQ0UTIL , který je zdokumentován v tématu Obslužný program zásad zabezpečení zpráv (CSQ0UTIL).

Obslužný program CSQ0UTIL použijte ke spuštění následujícího příkazu:

```
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 je 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 aktualizujte konfiguraci zásad produktu Advanced Message Security pomocí příkazu z/OS **MODIFY** . Příklad:

```
F BNK6AMSM,REFRESH POLICY
```

z/OS *Lokální ukládání zpráv chráněných soukromí do fronty pro AMS v systému z/OS*

Tento příklad podrobně popisuje zásady a certifikáty produktu Advanced Message Security potřebné k odesílání a načítání zpráv chráněných soukromě do fronty a z fronty, která je lokální vzhledem k ukládání a získávání aplikací. Zprávy chráněné heslem jsou podepsané i šifrované.

Ukázkový správce front a lokální fronta jsou následující:

```
BNK6        - Queue manager
FIN.XFER.Q8 - Local queue
```

Tito uživatelé se používají:

```
WMQBNK6  - AMS task user
TELLER5  - Sending user
FINADM2  - Recipient user
```

Postup konfigurace tohoto scénáře:

Vytvoření uživatelských certifikátů

V tomto příkladu se požadují dva uživatelské certifikáty. Jedná se o odesílaný uživatelský certifikát, který je nutný pro podepisování zpráv, a certifikát uživatele příjemce, který je potřebný pro šifrování a dešifrování dat zprávy. Odesílající uživatel je 'TELLER5' a uživatel příjemce je 'FINADM2'.

Je také požadován certifikát vydavatele certifikátů (CA).Certifikát CA je certifikát autority, která vydala certifikát uživatele. Může se jednat o řetězec certifikátů. Je-li tomu tak, 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 RACDCERT produktu RACF . 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 vydávání 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 procedury pro výběr nebo vytvoření certifikátu CA, stejně jako procedury pro vydávání certifikátů a distribuci těchto certifikátů do příslušných systémů.

Při exportu a importu těchto certifikátů produkt Advanced Message Security vyžaduje:

- Certifikát CA (řetězec).
- Odesílající uživatelský certifikát a jeho soukromý klíč.
- Certifikát uživatele příjemce a jeho soukromý klíč.

Používáte-li produkt RACF, lze příkaz RACDCERT EXPORT použít k exportování certifikátů do datové sady a příkaz RACDCERT ADD lze použít k importování certifikátů z datové sady. Další informace o těchto a dalších příkazech RACDCERT naleznete v tématu RACDCERT (Správa digitálních certifikátů RACF) v příručce *z/OS: Security Server RACF Command Language Reference*.

Certifikáty v tomto případě jsou vyžadovány na systému z/OS se spuštěným správcem front BNK6.

Pokud byly certifikáty importovány do systému z/OS se systémem BNK6, uživatelské certifikáty vyžadují atribut TRUST. Příkaz RACDRCERT ALTER lze použít k přidání atributu TRUST do certifikátu. Příklad:

```
RACDCERT ID(TELLER5) ALTER (LABEL('Teller5')) TRUST
RACDCERT ID(FINADM2) ALTER (LABEL('FinAdm2')) TRUST
```

Připojení certifikátů k příslušným klíčovým sdružením

Pokud byly požadované certifikáty vytvořeny nebo importovány a nastaveny jako důvěryhodné, musí být připojeny k příslušným prstenům klíčů uživatele na systému z/OS , kde je spuštěna 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 svazek klíčů pro odesílající a přijímající uživatele. Mějte na zřeteli, že název svazku klíčů drq.ams.keyring je povinný a název rozlišuje velká a malá písmena.

Když byly vytvořeny svazky klíčů, mohou být příslušné certifikáty připojeny.

```
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. Má-li uživatel více než jeden certifikát ve svém souboru drq.ams.keyring, použije se výchozí certifikát pro podepisování a pro účely dešifrování.

Certifikát uživatele příjemce musí být také připojen ke klíčovém okruhu uživatele úlohy Advanced Message Security s USAGE (SITE). Důvodem je to, že úloha zabezpečení rozšířených zpráv potřebuje veřejný klíč příjemce při šifrování dat zprávy. USAGE (SITE) zabraňuje tomu, aby byl soukromý klíč přístupný v klíčovém kruhu.

Vytvoření a úprava certifikátů nejsou produktem Advanced Message Security rozpoznány, dokud není správce front zastaven a restartován, nebo se příkaz z/OS **MODIFY** používá k aktualizaci konfigurace certifikátu produktu Advanced Message Security . Příklad:

```
F BNK6AMSM,REFRESH KEYRING
```

Vytvoření zásady produktu Advanced Message Security

V tomto příkladu jsou zprávy chráněné soukromě vloženy do fronty FIN.XFER.Q8 z aplikace spuštěné jako uživatel 'TELLER5' a načtené ze stejné fronty aplikací spuštěnými jako uživatel 'FINADM2', takže je vyžadována pouze jedna zásada Advanced Message Security .

Zásady produktu Advanced Message Security se vytvářejí pomocí obslužného programu CSQ0UTIL , který je zdokumentován v tématu Obslužný program zásad zabezpečení zpráv (CSQ0UTIL).

Obslužný program CSQ0UTIL použijte ke spuštění následujícího příkazu:

```
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 je FIN.XFER.Q8. Algoritmus použitý ke generování podpisu odesílatele je SHA1a rozlišující název (DN) odesílajícího uživatele je 'CN=Teller5,O=BCO,C=US' a uživatel příjemce je 'CN=FinAdm2,O=BCO,C=US'. Algoritmus, který se používá k šifrování dat zprávy, je 3DES.

Po definování zásady buď restartujte správce front BNK6 , nebo aktualizujte konfiguraci zásad produktu Advanced Message Security pomocí příkazu z/OS **MODIFY** . Příklad:

```
F BNK6AMSM,REFRESH POLICY
```

z/OS *Vzdálené ukládání zpráv chráněných proti integritě do fronty pro AMS v systému z/OS*

Tento příklad podrobně popisuje zásady a certifikáty produktu Advanced Message Security potřebné k odesílání a načítání zpráv chráněných integritou a z front spravovaných dvěma různými správci front. Dva správci front mohou být spuštění ve stejném systému z/OS nebo v různých systémech z/OS , nebo jeden správce front může být na distribuovaném systému, na kterém běží Advanced Message Security.

Příklad 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 spuštěni na různých systémech z/OS .

Tito uživatelé se používají:

```
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:

Vytvoření uživatelských certifikátů

V tomto příkladu je potřeba pouze jeden uživatelský certifikát. Jedná se o certifikát pro odeslání uživatele, který je nutný k podpisu zprávy chráněné integrity. Odesílající uživatel je 'TELLER5'.

Je také požadován certifikát vydavatele certifikátů (CA).Certifikát CA je certifikát autority, která vydala certifikát uživatele. Může se jednat o řetězec certifikátů. Je-li tomu tak, všechny certifikáty v řetězci jsou vyžadovány v svazku klíčů uživatele úlohy Advanced Message Security , v tomto případě uživatele WMQBNK7.

Certifikát CA lze vytvořit pomocí příkazu RACDCERT produktu RACF . 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 procedury pro výběr nebo vytvoření certifikátu CA, stejně jako procedury pro vydávání certifikátů a distribuci těchto certifikátů do příslušných systémů.

Při exportu a importu těchto certifikátů produkt Advanced Message Security vyžaduje:

- Certifikát CA (řetězec).
- Odesílající uživatelský certifikát a jeho soukromý klíč.

Používáte-li produkt RACF, lze příkaz RACDCERT EXPORT použít k exportování certifikátů do datové sady a příkaz RACDCERT ADD lze použít k importování certifikátů z datové sady. Další informace o těchto a dalších příkazech RACDCERT naleznete v tématu RACDCERT (Správa digitálních certifikátů RACF) v příručce *z/OS: Security Server RACF Command Language Reference*.

Certifikáty v tomto případě jsou vyžadovány na systému z/OS se spuštěným správcem front BNK6 a BNK7.

V tomto příkladu musí být odesílající certifikát importován na systému z/OS se systémem BNK6a certifikát CA musí být importován na systému z/OS spouštějícím BNK7. Když certifikáty byly importovány, uživatelský certifikát vyžaduje atribut TRUST. Příkaz RACDRCERT ALTER lze použít k přidání atributu TRUST do certifikátu. Například na BNK6:

```
RACDCERT ID(TELLER5) ALTER (LABEL('Teller5')) TRUST
```

Připojení certifikátů k příslušným klíčovým sdružením

Pokud byly požadované certifikáty vytvořeny nebo importovány a nastaveny jako důvěryhodné, musí být připojeny k příslušným prstenům klíčů uživatele na systému z/OS s operačním systémem 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 odeslání uživatele na BNK6. Mějte na zřeteli, že název svazku klíčů drq.ams.keyring je povinný a název rozlišuje velká a malá písmena.

V BNK7:

```
RACDCERT ID(WMQBNK7) ADDRING(drq.ams.keyring)
```

Tím se vytvoří klíčový kroužek pro uživatele úlohy Advanced Message Security na BNK7. Pro 'TELLER5' na BNK7není požadován žádný svazek klíčů uživatele.

Když byly vytvořeny svazky klíčů, mohou být příslušné certifikáty připojeny.

Dne BNK6:

```
RACDCERT ID(TELLER5) CONNECT(ID(TELLER5) LABEL('Teller5')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
```

V BNK7:

```
RACDCERT ID(WMQBNK7) CONNECT(CERTAUTH LABEL('BCOCA')
RING(drq.ams.keyring))
```

Odesílající se certifikát uživatele musí být připojen jako VÝCHOZÍ. Pokud má odesílající uživatel více než jeden certifikát ve svém souboru drq.ams.keyring, použije se výchozí certifikát pro účely podepisování.

Vytvoření a úprava certifikátů nejsou produktem Advanced Message Security rozpoznány, dokud není správce front zastaven a restartován, nebo se příkaz z/OS **MODIFY** používá k aktualizaci konfigurace certifikátu produktu Advanced Message Security . Příklad:

Dne BNK6:

```
F BNK6AMSM,REFRESH,KEYRING
```

V BNK7:

```
F BNK7AMSM,REFRESH,KEYRING
```

Vytvoření zásad produktu Advanced Message Security

V tomto příkladu jsou zprávy chráněné integrity vloženy do vzdálené fronty FIN.XFER.Q7 na BNK6 aplikací spuštěnou jako uživatel 'TELLER5' a načtené z lokální fronty FIN.RCPT.Q7 na BNK7 aplikací spuštěnou jako uživatel 'FINADM2', takže jsou vyžadovány dvě zásady Advanced Message Security .

Zásady produktu Advanced Message Security se vytvářejí pomocí obslužného programu CSQ0UTIL , který je zdokumentován v tématu Obslužný program zásad zabezpečení zpráv (CSQ0UTIL).

Použijte obslužný program CSQ0UTIL ke spuštění následujícího příkazu pro definování zásady integrity pro vzdálenou frontu na 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 je FIN.XFER.Q7. Algoritmus použitý ke generování podpisu odesílatele je MD5a rozlišující název (DN) odesílajícího uživatele je 'CN=Teller5,O=BCO,C=US'.

Použijte také obslužný program CSQ0UTIL a spusťte následující příkaz k definování zásady integrity pro lokální frontu na 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 je FIN.RCPT.Q7. Algoritmus očekávaný 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 restartujte správce front BNK6 a BNK7 nebo pomocí příkazu z/OS **MODIFY** aktualizujte konfigurace zásad produktu Advanced Message Security . Příklad:

Dne BNK6:

```
F BNK6AMSM,REFRESH,POLICY
```

V BNK7:

```
F BNK7AMSM,REFRESH,POLICY
```

z/OS *Vzdálené ukládání zpráv chráněných ochranou soukromí pro produkt AMS v systému z/OS*
Tento příklad podrobně popisuje zásady a certifikáty produktu Advanced Message Security potřebné k odesílání a načítání zpráv chráněných soukromě a z front spravovaných dvěma různými správci front. Dva správci front mohou být spuštění ve stejném systému z/OS nebo v různých systémech z/OS , nebo jeden správce front může být na distribuovaném systému, na kterém běží Advanced Message Security.

Příklad 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 správci front BNK6 a BNK7 správci front spuštěni na různých systémech z/OS se stejným názvem.

Tito uživatelé se používají:

```
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:

Vytvoření uživatelských certifikátů

V tomto příkladu se požadují dva uživatelské certifikáty. Jedná se o odesílaný uživatelský certifikát, který je nutný pro podepisování zpráv, a certifikát uživatele příjemce, který je potřebný pro šifrování a dešifrování dat zprávy. Odesílající uživatel je 'TELLER5' a uživatel příjemce je 'FINADM2'.

Je také požadován certifikát vydavatele certifikátů (CA).Certifikát CA je certifikát autority, která vydala certifikát uživatele. Může se jednat o řetězec certifikátů. Je-li tomu tak, všechny certifikáty v řetězci jsou vyžadovány v svazku klíčů uživatele úlohy Advanced Message Security , v tomto případě uživatele WMQBNK7.

Certifikát CA lze vytvořit pomocí příkazu RACDCERT produktu RACF . 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 vydávání 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 procedury pro výběr nebo vytvoření certifikátu CA, stejně jako procedury pro vydávání certifikátů a distribuci těchto certifikátů do příslušných systémů.

Při exportu a importu těchto certifikátů produkt Advanced Message Security vyžaduje:

- Certifikát CA (řetězec).
- Odesílající uživatelský certifikát a jeho soukromý klíč.
- Certifikát uživatele příjemce a jeho soukromý klíč.

Používáte-li produkt RACF, lze příkaz RACDCERT EXPORT použít k exportování certifikátů do datové sady a příkaz RACDCERT ADD lze použít k importování certifikátů z datové sady.

Další informace o těchto a dalších příkazech RACDCERT naleznete v části RACDCERT (Správa digitálních certifikátů RACF) v příručce *z/OS: Security Server RACF Command Language Reference*.

Certifikáty v tomto případě jsou vyžadovány na systému z/OS se spuštěným správcem front BNK6 a BNK7.

V tomto příkladu musí být odesílající a přijímající certifikáty importovány na systém z/OS s operačním systémem BNK6a certifikáty CA a příjemce musí být importovány do systému z/OS , kde je spuštěna BNK7. Když certifikáty byly importovány, uživatelské certifikáty vyžadují atribut TRUST. Příkaz RACDRCERT ALTER lze použít k přidání atributu TRUST do certifikátu. Příklad:

Dne BNK6:

```
RACDCERT ID(TELLER5) ALTER (LABEL('Teller5')) TRUST
RACDCERT ID(FINADM2) ALTER (LABEL('FinAdm2')) TRUST
```

V BNK7:

```
RACDCERT ID(FINADM2) ALTER (LABEL('FinAdm2')) TRUST
```

Připojení certifikátů k příslušným klíčovým sdružením

Pokud byly požadované certifikáty vytvořeny nebo importovány a nastaveny jako důvěryhodné, musí být připojeny k příslušným klíčům uživatelských klíčů na systémech z/OS s operačním systémem BNK6 a BNK7.

Chcete-li vytvořit svazky klíčů, použijte příkaz RACDCERT ADDRING:

Dne 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 odeslání uživatele na BNK6. Mějte na zřeteli, že název svazku klíčů drq.ams.keyring je povinný a název rozlišuje velká a malá písmena.

V 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 BNK7.

Když byly vytvořeny svazky klíčů, mohou být příslušné certifikáty připojeny.

Dne 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))
```

V 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. Má-li uživatel více než jeden certifikát ve svém souboru drq.ams.keyring, použije se výchozí certifikát pro podepisování a pro účely šifrování/dešifrování.

V případě BNK6musí být certifikát uživatele příjemce také připojen ke klíčovém okruhu uživatele úlohy Advanced Message Security s USAGE (SITE). Důvodem je to, že úloha zabezpečení rozšířených zpráv potřebuje veřejný klíč příjemce při šifrování dat zprávy. USAGE (SITE) zabraňuje tomu, aby byl soukromý klíč přístupný v klíčovém kruhu.

Vytvoření a úprava certifikátů nejsou produktem Advanced Message Security rozpoznány, dokud není správce front zastaven a restartován, nebo se příkaz z/OS **MODIFY** používá k aktualizaci konfigurace certifikátu produktu Advanced Message Security . Příklad:

Dne BNK6:

```
F BNK6AMSM,REFRESH,KEYRING
```

V BNK7:

```
F BNK7AMSM,REFRESH,KEYRING
```

Vytvoření zásad produktu Advanced Message Security

V tomto příkladu jsou zprávy chráněné soukromě vloženy do vzdálené fronty FIN.XFER.Q7 na BNK6 aplikací spuštěnou jako uživatel 'TELLER5' a načtené z lokální fronty FIN.RCPT.Q7 na BNK7 aplikací spuštěnou jako uživatel 'FINADM2', takže jsou vyžadovány dvě zásady Advanced Message Security .

Zásady produktu Advanced Message Security se vytvářejí pomocí obslužného programu CSQ0UTIL , který je zdokumentován v tématu Obslužný program zásad zabezpečení zpráv (CSQ0UTIL).

Použijte obslužný program CSQ0UTIL pro spuštění následujícího příkazu k definování zásady ochrany osobních údajů pro vzdálenou frontu na 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 je FIN.XFER.Q7. Algoritmus použitý ke generování podpisu odesílatele je SHA1, rozlišující název (DN) odesílajícího uživatele je 'CN=Teller5,O=BCO,C=US' a uživatel příjemce je 'CN=FinAdm2,O=BCO,C=US'. Algoritmus, který se používá k šifrování dat zprávy, je 3DES.

Použijte také obslužný program CSQ0UTIL a spusťte následující příkaz k definování zásady ochrany osobních údajů pro lokální frontu na 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 je FIN.RCPT.Q7. Algoritmus očekávaný pro podpis odesílatele je 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, který se používá k dešifrování dat zprávy, je 3DES.

Po definování těchto dvou zásad restartujte správce front BNK6 a BNK7 , nebo pomocí příkazu z/OS **MODIFY** obnovte konfiguraci zásady produktu Advanced Message Security . Příklad:

Dne BNK6:

```
F BNK6AMSM,REFRESH,POLICY
```

V BNK7:

```
F BNK7AMSM,REFRESH,POLICY
```

Stručná úvodní příručka pro AMS s klienty Java

Pomocí této příručky můžete rychle nakonfigurovat produkt Advanced Message Security a poskytnout zabezpečení zpráv pro aplikace produktu Java , které se připojují pomocí vazeb klienta. Po dokončení tohoto procesu jste vytvořili úložiště klíčů k ověření identit uživatelů a definované zásady pro podepisování a šifrování pro 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 místě, ve kterém vstupují do infrastruktury produktu IBM MQ prostřednictvím standardního rozhraní produktu IBM MQ . Základní nastavení se provádí v produktu IBM MQ a je konfigurováno 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 produktu **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 naše aplikace k připojení zadáním následujícího příkazu do produktu **runmqsc** pro správce front QM_VERIFY_AMS

   ```
   DEFINE CHANNEL(AMS.SVRCONN) CHLTYPE(SVRCONN)
   ```

5. Vytvořte frontu s názvem TEST.Q zadáním následujícího příkazu do produktu **runmqsc** pro správce front QM_VERIFY_AMS

   ```
   DEFINE QLOCAL(TEST.Q)
   ```

Výsledky

Pokud byla procedura úspěšně dokončena, následující příkaz zadaný do produktu **runmqsc** zobrazí podrobnosti o produktu TEST.Q:

```
DISPLAY Q(TEST.Q)
```

2. Vytvoření a autorizace uživatelů

Informace o této úloze

Existují dva uživatelé, kteří se zobrazí v tomto scénáři: `alice`, odesílatel a bob, příjemce. K tomu, abyste mohli používat aplikační frontu, je třeba těmto uživatelům udělit oprávnění k jeho používání. 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** naleznete v části **setmqaut**.

Postup

1. Vytvořte dva uživatele, jak je popsáno v příručce **Quick Start Guide** (Windows nebo AIX and Linux) pro vaši platformu.
2. Autorizovat uživatele pro připojení ke správci front a pro práci s touto 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 povolit, aby dva uživatelé procházeli frontu zásad systému a vložili 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 pomocí zásad ukládání do mezipaměti, takže nemusíte procházet záznamy o podrobnostech zásady v systému SYSTEM.PROTECTION.POLICY.QUEUE ve všech případech.

   Produkt IBM MQ neukládá do mezipaměti všechny dostupné zásady. Existuje-li vysoký počet zásad, produkt IBM MQ ukládá omezený počet zásad do mezipaměti. Má-li tedy správce front definován nízký počet definovaných zásad, není třeba zadávat volbu procházení do systému SYSTEM.PROTECTION.POLICY.QUEUE.

   Do této fronty byste však měli udělit oprávnění k procházení, v případě, že je definován vysoký počet zásad, nebo pokud používáte staré klienty. SYSTEM.PROTECTION.ERROR.QUEUE se používá k vložení chybových zpráv generovaných kódem AMS. Oprávnění k vložení pro tuto frontu se kontroluje pouze tehdy, když se pokusíte vložit chybovou zprávu do fronty. Při pokusu o vložení nebo získání zprávy z chráněné fronty AMS se nekontroluje vaše oprávnění k zařazení do fronty.

Výsledky

Uživatelé jsou nyní vytvořni a požadovaná oprávnění jim byla udělena.

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 616.

3. Vytvoření databáze klíčů a certifikátů

Informace o této úloze

Chcete-li zašifrovat zprávu zachytávačem, je nutný veřejný klíč odesílajícího uživatele. Proto musí být vytvořena klíčová databáze identit uživatelů namapovaných na veřejné a soukromé klíče. V reálném systému, kde uživatelé a aplikace jsou rozptýleni přes několik počítačů, by měl každý uživatel své vlastní soukromé úložiště klíčů. Podobně v této příručce vytváříme databáze klíčů pro `alice` a bob a sdílíme uživatelské certifikáty mezi nimi.

Poznámka: V této příručce se používají ukázkové aplikace napsané v produktu Java , které se připojují pomocí vazeb klienta. Plánujete-li používat aplikace produktu Java s použitím lokálních vazeb nebo aplikací v jazyce C, je nutné vytvořit úložiště klíčů a certifikáty CMS pomocí příkazu **runmqakm** . To se zobrazí v **Stručné úvodní příručce** (Windows nebo AIX and Linux).

Postup

1. Vytvořte adresář, ve kterém chcete vytvořit úložiště klíčů, například `/home/alice/.mqs`. Možná si ji budete přát vytvořit ve stejném adresáři, jaký používá **Stručná úvodní příručka** (Windows nebo AIX and Linux) pro vaši platformu.

   Poznámka: Tento adresář je označován jako *keystore-dir* v následujících krocích
2. Vytvoření nového úložiště klíčů a certifikátu identifikujícího 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 adresář *keystore-dir* obsahuje mezery, je třeba zadat úplný název úložiště klíčů do uvozovek.
   - Je vhodné použít silné heslo k zabezpečení úložiště klíčů.
   - Pro účely této příručky používáme certifikát podepsaný držitelem, který může být vytvořen bez použití certifikační autority. U výrobních systémů se doporučuje nepoužívat certifikáty podepsané sebou samým, ale spíše spoléhat na certifikáty podepsané vydavatelem certifikátů.
   - Parametr **alias** určuje název certifikátu, který zachytávače vyhledají, aby obdrželi potřebné informace.
   - Parametr **dname** určuje podrobnosti o **rozlišujícím názvu** (DN), které musí být jedinečné pro každého uživatele.
3. V systému AIX and Linuxzkontrolujte, zda je úložiště klíčů čitelné.

   ```
   chmod +r keystore-dir/keystore.jks
   ```
4. Zopakovat step1-4 pro uživatele bob

Výsledky

Dva uživatelé `alice` a bob mají každý nyní certifikát podepsaný svým držitelem.

4. Vytvoření souboru keystore.conf

Informace o této úloze

Do adresáře, kde jsou umístěny databáze klíčů a certifikáty, musíte zabodávat zachytávače Advanced Message Security . To se provádí pomocí souboru `keystore.conf` , který uchovává tyto informace ve formě prostého textu. Každý uživatel musí mít samostatný soubor `keystore.conf` . Tento krok by měl být proveden pro `alice` i pro bob.

Příklad

Pro tento scénář je obsah souboru `keystore.conf` pro produkt `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 souboru `keystore.conf` pro produkt 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 příručce Quick Start Guide (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 625.

5. Sdílení certifikátů

Informace o této úloze

Sdílejte certifikáty mezi dvěma úložišti klíčů tak, aby každý uživatel mohl úspěšně identifikovat ostatní. To se provádí extrahováním certifikátu každého uživatele a jeho importem do úložiště klíčů jiného uživatele.

Poznámka: Termíny *extract* a *export* se používají rozdílně různými nástroji certifikátů. Nástroj IBM GSKit **strmqikm** (nástroj ikeyman) například rozlišuje, že jste *extrahovali* certifikáty (veřejné klíče) a soukromé klíče *exportu* . Tento rozdíl je nesmírně důležitý pro nástroje, které nabízejí obě možnosti, protože používání *exportu* omylem zcela kompromituje vaši aplikaci předáním svého soukromého klíče. Protože je rozdíl natolik důležitý, snaží se dokumentace produktu IBM MQ důsledně používat tyto termíny. Nástroj keytool produktu Java však poskytuje volbu příkazového řádku s názvem *exportcert* , která extrahuje pouze veřejný klíč. Z těchto důvodů se následující procedura odkazuje na *extrahování* certifikátů pomocí volby *exportcert* .

Postup

1. Extrahujte certifikát označující `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, který identifikuje produkt `alice` , do úložiště klíčů, které bude používat produkt bob . Až budete vyzváni, označte, že tomuto certifikátu důvěřujete.

   ```
   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 navzájem úspěšně identifikovat, protože vytvořili a sdíleli certifikáty podepsané sebou samým.

Jak pokračovat dále

Spuštěním následujících příkazů, které vytisknou jeho podrobnosti, ověřte, že je certifikát v úložišti klíčů:

```
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

Se správcem front vytvořeným a zachytávačem připraveným k zachycení zpráv a přístupu k šifrovacím klíčům můžeme začít definovat zásady ochrany na systému QM_VERIFY_AMS pomocí příkazu `setmqspl` . Další informace o tomto příkazu najdete v souboru setmqspl . Každý název zásady musí být stejný jako název fronty, na který se má použít.

Příklad

Toto je příklad zásady definované ve frontě `TEST.Q` , která je podepsána uživatelem `alice` pomocí algoritmu SHA1 a šifrována 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 certifikátu příslušného uživatele od 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` , parametr `-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 jazyka Java, kterou používáte, má nainstalované neomezené soubory zásad JCE.

Poznámka: Verze jazyka Java dodaná v instalaci produktu IBM MQ již má tyto soubory zásad. Lze jej nalézt v *MQ_INSTALLATION_PATH*`/java/bin`.

Informace o této úloze

Spuštěním různých programů pod různými uživateli můžete ověřit, zda byla aplikace řádně nakonfigurována. Podrobnosti o spouštění programů pod různými uživateli najdete v příručce **Quick Start Guide** (Windows nebo AIX).

Postup

1. Chcete-li spustit tyto ukázkové aplikace produktu JMS , použijte nastavení CLASSPATH pro vaši platformu, jak je zobrazeno v tématu Proměnné prostředí používané produktem IBM MQ classes for JMS k zajištění toho, aby byl zahrnut adresář ukázek.
2. Jako uživatel `alice`vložte zprávu s použitím ukázkové aplikace, která se připojuje jako klient:

```
java JmsProducer -m QM_VERIFY_AMS -d TEST.Q -h localhost -p 1414 -l AMS.SVRCONN
```

3. Jako uživatel bobzískám 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 aplikaci získání.

Ochrana vzdálených front v systému AMS

Aby bylo možné plně chránit vzdálené fronty, musí být nastaveny zásady na vzdálené frontě a lokální frontě, do které jsou zprávy přenášeny.

Když je zpráva vložena do vzdálené fronty, produkt Advanced Message Security zadrží operaci a zpracuje zprávu na základě sady zásad pro vzdálenou frontu. Například pro zásadu šifrování je zpráva zašifrována před tím, než je předána procesu IBM MQ , aby se s ní ošetla. Poté, co příkaz Advanced Message Security zpracoval zprávu vdanou do vzdálené fronty, vloží příkaz IBM MQ do přidružené přenosové fronty a předá ji cílovému správci front a cílové frontě.

Je-li operace GET provedena v lokální frontě, 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 s tím, která byla použita k zašifrování. Jakýkoli nesoulad způsobí, že zpráva bude odmítnuta.

Pokud z nějakého důvodu nemohou být obě zásady nastaveny současně, je poskytována podpora fázovaného nasazení. Zásada může být nastavena na lokální frontě s příznakem tolerování, což znamená, že zásada přidružená k frontě může být ignorována, když se pokus o načtení zprávy z fronty zahrnuje zprávu, která nemá nastavovanou sadu zásad zabezpečení. V takovém případě se metoda GET pokusí dešifrovat zprávu, ale umožní doručení nešifrovaných zpráv. Takto mohou být zásady vzdálených front nastaveny po ochraně lokálních front (a testování).

Zapamatujte si: Jakmile je dokončeno ukončení Advanced Message Security , odeberte příznak tolerance.

Související odkazy

setmqspl (nastavit zásady zabezpečení)

Směrování chráněných zpráv pomocí AMS pomocí IBM Integration Bus

Produkt Advanced Message Security může ochraňovat zprávy v infrastruktuře, kde je nainstalován produkt IBM Integration Busnebo produkt WebSphere Message Broker 8.0.0.1 (nebo novější). Před použitím zabezpečení v prostředí produktu IBM Integration Bus byste měli porozumět povaze obou produktů.

Informace o této úloze

Advanced Message Security poskytuje konec pro zabezpečení informačního obsahu zprávy. To znamená, že pouze účastníci uvedení jako platní odesilatelé a příjemci zprávy jsou schopni produkovat nebo přijímat. To znamená, že za účelem zabezpečení zpráv procházejících přes IBM Integration Busmůžete buď povolit IBM Integration Bus ke zpracování zpráv, aniž byste znali jejich obsah (Scénář 1) nebo jej zpřístupníte autorizovaným uživatelem pro příjem a odesílání zpráv (Scénář 2).

Scénář 1- Integration Bus nemůže zobrazit obsah zprávy

Než začnete

Měli byste mít IBM Integration Bus připojený ke stávajícímu správci front. Řetězec *QMgrName* nahraďte tímto existujícím názvem správce front v následujících příkazech.

Informace o této úloze

V tomto scénáři Alice umístí chráněnou zprávu do vstupní fronty QIN. Na základě vlastnosti zprávy routeToje zpráva směrována buď na *bob's* (QBOB),[1](QCECIL) nebo výchozí fronty (QDEF). Směrování je možné, protože Advanced Message Security chrání pouze informační obsah zprávy a ne jeho záhlaví a vlastnosti, které zůstávají nechráněné a mohou být čteny IBM Integration Bus. Produkt Advanced Message Security používá pouze *alice*, *bob* a *cecil*. Není nutné ji instalovat nebo konfigurovat pro produkt IBM Integration Bus.

Produkt IBM Integration Bus přijme chráněnou zprávu z nezabezpečené fronty aliasů, aby nedošlo k pokusu o dešifrování zprávy. Pokud by se jednalo o přímé použití chráněné fronty, zpráva by byla vložena do fronty DEAD LETTER jako nemožnou k dešifrování. Zpráva je směrována IBM Integration Bus a je doručena do cílové fronty nezměněná. Proto je i nadále podepsán původním autorem (oba *bob* a *cecil* přijímají pouze zprávy odeslané *alice*) a chráněné jako předtím (pouze *bob* a *cecil* mohou číst). Příkaz IBM Integration Bus vloží přesměrovanou 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 produktu Advanced Message Security , jak je popsáno v příručce **Quick Start Guide** (Windows nebo AIX).

   Ujistěte se, že jsou dokončeny následující kroky:

   - Vytvoření a autorizace uživatelů
   - Vytvoření databáze klíčů a certifikátů
   - Vytvoření souboru keystore.conf
2. Poskytněte certifikát *alice* pro *bob* a *cecil*, takže *alice* je možné identifikovat při kontrole digitálních podpisů na zprávách.

   To provedete extrahováním certifikátu identifikujícího *alice* do externího souboru a následným přidáním extrahovaného certifikátu do úložišť klíčů *bob* a *cecil* . Je důležité, abyste použili metodu popsanou v **Úloha 5. Sdílení certifikátů** v příručce **Quick Start Guide** (Windows nebo AIX).
3. Zadejte certifikáty *bob* a *cecil* do *alice*, takže *alice* může odesílat zprávy zašifrované pro *bob* a *cecil*.

   Postupujte takto s použitím metody uvedené v předchozím kroku.
4. V daném správci front definujte lokální fronty s názvem QIN, QBOB, QCECIL a QDEF.

   ```
   DEFINE QLOCAL(QIN)
   ```
5. Nastavte zásady zabezpečení pro frontu QIN na vhodnou konfiguraci. Použijte identické nastavení pro fronty QBOB, QCECIL a QDEF .

   ```
   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 jediný autorizovaný odesilatel a *bob* a *cecil* jsou příjemci.
6. Definujte aliasy front AIN, ABOB a ACECIL odkazující na lokální fronty QIN, QBOB a QCECIL .

   ```
   DEFINE QALIAS(AIN) TARGET(QIN)
   ```
7. Ověřte, že konfigurace zabezpečení pro aliasy uvedené v předchozím kroku není přítomna; jinak nastavte její zásadu na NONE.

   ```
   dspmqspl -m QMgrName -p AIN
   ```

[1] cecil

8. V produktu IBM Integration Bus vytvořte tok zpráv pro směrování zpráv, které přicházejí do fronty aliasů AIN , do uzlu BOB, CECIL nebo DEF v závislosti na vlastnosti routeTo zprávy. Chcete-li to provést:
   a) Vytvořte uzel MQInput s názvem IN a přiřaďte mu alias AIN jako název fronty.
   b) Vytvořte uzly MQOutput s názvem BOB, CECIL a DEFa přiřaďte aliasy front ABOB, ACECIL a ADEF jako příslušné názvy front.
   c) Vytvořte uzel přenosové cesty a nazte 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 produktu IBM Integration Bus .
10. Spuštění jako uživatel Alice vložil zprávu, která také obsahuje vlastnost zprávy s názvem routeTo s hodnotou buď bob , nebo cecil. Spuštění ukázkové aplikace **amqsstm** vám umožní toto provést.

```
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. Při spuštění jako uživatel *bob* načtěte zprávu z fronty QBOB s použitím ukázkové aplikace **amqsget**.

Výsledky

Když text *alice* vloží zprávu do fronty QIN , je zpráva chráněna. Je načten v chráněné formě produktem IBM Integration Bus z alias fronty AIN . IBM Integration Bus rozhoduje o tom, kam směrovat zprávu při čtení vlastnosti routeTo , která je jako všechny vlastnosti nešifrována. Produkt IBM Integration Bus umístí zprávu na příslušný nechráněný alias, aby se zabránilo jeho další ochraně. Při přijetí od *bob* nebo *cecil* z fronty je zpráva dešifrována a digitální podpis je ověřen.

Scénář 2- Integration Bus může zobrazit obsah zprávy

Informace o této úloze

V tomto scénáři je skupině jednotlivců povoleno odesílat zprávy do produktu IBM Integration Bus. Jiná skupina je oprávněna přijímat zprávy, které jsou vytvořeny produktem IBM Integration Bus. Přenos mezi stranami a IBM Integration Bus nemůže být odposlouchněný.

Pamatujte, že produkt IBM Integration Bus čte zásady ochrany a certifikáty pouze při otevření fronty, takže musíte znovu načíst skupinu provádění po provedení jakýchkoli aktualizací zásad ochrany, aby změny nabyly platnosti.

```
mqsireload execution-group-name
```

Je-li produkt IBM Integration Bus považován za autorizovanou stranu, která má oprávnění ke čtení nebo podepsání informačního obsahu zprávy, musíte nakonfigurovat prostor Advanced Message Security pro

uživatele spouštějícího službu IBM Integration Bus . Mějte na paměti, že se nejedná nutně o stejného uživatele, který vkládá/získává zprávy do front, ani uživatele, který vytváří a implementuje aplikace produktu IBM Integration Bus .

Postup

1. Nakonfigurujte *alice*, *bob*, *cecil* a *dsave* a uživatele služby IBM Integration Bus , abyste mohli použít produkt Advanced Message Security , jak je popsáno v příručce **Quick Start Guide** (Windows nebo AIX).

   Ujistěte se, že jsou dokončeny následující kroky:

   - Vytvoření a autorizace uživatelů
   - Vytvoření databáze klíčů a certifikátů
   - Vytvoření souboru keystore.conf
2. Zadejte certifikáty *alice*, *bob*, *cecil* a *dave* uživateli služeb produktu IBM Integration Bus .

   To provedete extrakcí každého z certifikátů, které identifikují *alice*, *bob*, *cecil* a *dave* , do externích souborů a poté přidají extrahované certifikáty do úložiště klíčů produktu IBM Integration Bus . Je důležité, abyste použili metodu popsanou v **Úloha 5. Sdílení certifikátů** v příručce **Quick Start Guide** (Windows nebo AIX).
3. Zadejte certifikát uživatele služby IBM Integration Bus do *alice*, *bob*, *cecil* a *dave*.

   Postupujte takto s použitím metody uvedené v předchozím kroku.

   Poznámka: *Alice* a *bob* potřebují certifikát uživatele služby IBM Integration Bus , aby správně zašifrovali zprávy. Uživatel služby IBM Integration Bus potřebuje certifikáty *alice's* a *bob* k ověření autorů zpráv. Uživatel služby IBM Integration Bus potřebuje certifikáty *cecil's* a *dave* , aby pro ně šifroval zprávy. *cecil* a *dave* potřebují certifikát uživatele služby IBM Integration Bus , aby ověřil, zda zpráva pochází z produktu IBM Integration Bus.
4. Definujte lokální frontu s názvem `IN` a definujte zásadu zabezpečení s hodnotou *alice* a *bob* určeným jako autoři a uživatel služby pro IBM Integration Bus zadaný 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 `OUT`a definujte zásadu zabezpečení se servisním uživatelem pro IBM Integration Bus zadanou jako autor a *cecil* a *dave* uvedeným 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 `MQOutput` . Nakonfigurujte uzel `MQInput` pro použití fronty `IN` a uzlu `MQOutput` pro použití fronty `OUT` .
7. Implementujte tok zpráv do běhové komponenty produktu IBM Integration Bus .
8. Spuštění jako uživatel *alice* nebo *bob* vloží zprávu do fronty `IN` s použitím ukázkové aplikace **`amqsput`**.
9. Při spuštění jako uživatel *cecil* nebo *dave* načtěte zprávu z fronty `OUT` s použitím ukázkové aplikace **`amqsget`**.

Výsledky

Zprávy odeslané pomocí *alice* nebo *bob* do vstupní fronty `IN` jsou šifrovány tak, že je lze číst pouze IBM Integration Bus . Produkt IBM Integration Bus přijímá pouze zprávy od *alice* a *bob* a odmítá všechny ostatní. Přijímané zprávy jsou odpovídajícím způsobem zpracovány, pak jsou podepsány a šifrovány pomocí klíčů *cecil* a *dave* před tím, než jsou vloženy do výstupní fronty `OUT`. Pouze *cecil* a *dave* jsou schopny jej číst, zprávy, které nejsou podepsány IBM Integration Bus , jsou zamítnuty.

Použití Advanced Message Security s Managed File Transfer

Tento scénář vysvětluje, jak nakonfigurovat produkt Advanced Message Security , aby poskytoval důvěrnost dat pro data odesílaná prostřednictvím produktu Managed File Transfer.

Než začnete

Ujistěte se, že máte nainstalovanou komponentu Advanced Message Security na instalaci produktu IBM MQ hosting front použitých 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 GSKit na lokální instalaci.

Informace o této úloze

Je-li přenos dat mezi dvěma agenty Managed File Transfer přerušen, potenciálně důvěrné údaje mohou zůstat nechráněny na základních frontách produktu IBM MQ používaných ke správě přenosu. Tento scénář vysvětluje, jak nakonfigurovat a používat produkt Advanced Message Security k ochraně těchto dat ve frontách produktu Managed File Transfer .

V tomto scénáři uvažujeme jednoduchou topologii zahrnující jeden počítač se dvěma frontami Managed File Transfer a dvěma agenty, `AGENT1` a `AGENT2`a sdílením 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 je uživatel `ftagent` ve skupině `FTAGENTS` použit ke spouštění procesů Managed File Transfer Agent . 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 podpisu a/nebo šifrování zpráv v chráněných frontách.

Poznámka:

- Pokud jsou agenti Managed File Transfer spuštěni v režimu vazeb, příkazy, které používáte k vytvoření úložiště klíčů CMS (Cryptographic Message Syntax), jsou podrobně popsány v příručce **Quick Start Guide** (Windows nebo AIX) pro vaši platformu.
- Pokud jsou agenti Managed File Transfer spuštění v režimu klienta, příkazy, které budete potřebovat pro vytvoření JKS (Java Keystore), jsou podrobně popsány v “Stručná úvodní příručka pro AMS s klienty Java” na stránce 612.

Postup

1. Vytvořte certifikát podepsaný (svým) držitelem k identifikaci uživatele `ftagent` , jak je podrobně popsáno v příslušné stručné úvodní příručce.
   Rozlišovací jméno (DN) použijte následujícím způsobem:

   ```
   CN=ftagent, OU=MFT, O=<organisation>, L=<location>, ST=<state>, C=<country>
   ```

2. Vytvořte soubor `keystore.conf` pro identifikaci umístění úložiště klíčů a certifikátu v něm, jak je podrobně popsáno v příslušné stručné úvodní příručce.

2. Konfigurace ochrany zpráv

Informace o této úloze

Měli byste definovat zásady zabezpečení pro datovou frontu, kterou používá produkt AGENT2, pomocí příkazu **setmqspl** . V tomto scénáři je ke spuštění obou agentů použit stejný uživatel, a proto jsou podepisující a podpisový rozlišující název stejný a odpovídají certifikátu, který jsme vygenerovali.

Postup

1. Ukončete agenty Managed File Transfer v rámci přípravy na ochranu pomocí příkazu **fteStopAgent** .
2. Vytvoření zásad 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 spouští proces produktu Managed File Transfer Agent , má přístup k procházení fronty systémových zásad a k 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 úspěšné restartování agentů pomocí příkazu **fteListAgents** a ověření, že agenti jsou ve stavu READY .

Výsledky

Nyní můžete odesílat přenosy z AGENT1 do AGENT2a obsah souboru se bude přenášet zabezpečeně mezi dvěma agenty.

Advanced Message Security přehled instalace

Nainstalujte komponentu Advanced Message Security na různých platformách.

Procedura

- Nainstalujte produkt Advanced Message Security na více platformách.
- Nainstalujte produkt IBM MQ Advanced for z/OS.
- Nainstalujte produkt IBM MQ Advanced for z/OS Value Unit Edition.

Související úlohy

OdinstalaceAdvanced Message Security

z/OS Auditování pro AMS v systému z/OS

Advanced Message Security (AMS) for z/OS poskytuje prostředek pro volitelný audit operací aplikací v rámci front chráněných front. Je-li povolena tato volba, jsou generovány záznamy auditu SMF (System Management Facility) produktu IBM pro úspěch a selhání těchto operací ve frontách chráněných pojistek. Auditované operace zahrnují MQPUT, MQPUT1a MQGET.

Auditování je však standardně vypnuto, můžete aktivovat auditování konfigurací _AMS_SMF_TYPE a _AMS_SMF_AUDIT v konfigurovaném souboru jazykového 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 označení typu záznamu SMF a je číslo mezi 128 a 255. Záznam SMF typu 180 je obvykle běžný, avšak není povinný. Auditování je vypnuto uvedením hodnoty 0. Proměnná _AMS_SMF_AUDIT konfiguruje, zda jsou záznamy auditu vytvořeny pro operace, které jsou úspěšné, operace, které selžou, nebo obojí. Volby monitorování lze také dynamicky měnit, zatímco AMS je

aktivní pomocí příkazů operátora. Další informace najdete v tématu Provozní prostředí Advanced Message Security.

Záznam SMF je definován pomocí podtypů, přičemž podtyp 1 je obecnou událostí auditu. Záznam SMF obsahuje všechna data důležitá pro zpracovávaný požadavek.

Záznam SMF je mapován makrem CSQ0KSMF (všimněte si nulové hodnoty v názvu makra), který je poskytován v cílové knihovně SCSQMACS. Pokud zapisujete programy pro redukci dat pro data SMF, můžete toto makro mapování zahrnout do podpory při vývoji a přizpůsobení rutin následného zpracování SMF.

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 parametrem Advanced Message Security pro z/OS
- oddíl produktu
- datová sekce

Sekce produktu záznamu SMF je vždy prezentovaná v záznamech vytvořených produktem Advanced Message Security pro produkt z/OS. Datová sekce se liší v závislosti na podtypu. V současné době je definován jeden podtyp, a proto se používá jedna datová sekce.

Prostředí SMF je popsáno v příručce z/OS System Management Facilities (SA22-7630). Platné typy záznamů jsou popsány v členu SMFPRMxx vaší datové sady PARMLIB. Další informace naleznete v dokumentaci SMF.

Generátor sestav auditu Advanced Message Security (CSQ0USMF)

Produkt Advanced Message Security for z/OS poskytuje nástroj pro generování sestav auditu s názvem CSQ0USMF , který je poskytován v rámci instalace knihovny SCSQAUTH. Ukázkový kód JCL ke spuštění obslužného programu CSQ0USMF s názvem CSQ40RSM je k dispozici v instalační knihovně SCSQPROC.

Před spuštěním obslužného programu CSQ0USMF musí být záznamy SMF typu 180 vypisovány z systémových datových sad SMF do sekvenční datové sady. Jako příklad tento kód JCL 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 používané vaší instalací. Cílová datová sada pro dumpingové záznamy musí mít formát záznamu VBS a délku záznamu 32760.

Poznámka: Pokud se používají proudy protokolů SMF, musíte pomocí programu IFASMFDL vypsat proud protokolu do sekvenční datové sady. Příklad použitých JCL viz Zpracování typů 116 záznamů SMF .

Cílová datová sada může být poté použita jako vstup pro obslužný program CSQ0USMF , aby bylo možné vygenerovat sestavu 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 části Tabulka 101 na stránce 624:

Tabulka 101. Volitelné parametry CSQ0USMF		
Parametr	**Hodnota**	**Popis**
SMFTYP	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 parametr SMFTYPE, použije se výchozí hodnota 180.
M	QMGR	Název správce front produktu IBM MQ vhodný pro sestavu auditu. Nezadáte-li 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:

- IBM i Linux AIX V systému IBM i, AIX and Linux: `$HOME/.mqs/keystore.conf`
- Windows V systému Windows: *%HOMEDRIVE%%HOMEPATH%*`\.mqs\keystore.conf`

  Poznámka: Cesta v systému Windows může a měla by uvádět písmeno jednotky, pokud je k dispozici více než jedno písmeno jednotky.

Pokud používáte zadaný název souboru úložiště klíčů a umístění, měli byste použít následující příkazy

- 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`*

Ochrana citlivých informací v souboru `keystore.conf`

V 9.2.0 V 9.2.0

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 643 .

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.

Další informace viz "Advanced Message Security" na stránce 552.

Související pojmy

"Rozlišující názvy odesilatelů v souboru AMS" na stránce 651
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 653
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:

V 9.2.0 V 9.2.0 **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 Šifrovací šifrování RACF keyring KeyStore, konfigurační položky 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 pro non-IBM JRE s AMS" na stránce 630.

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 9.2.2 pkcs11.encrypted = no
```

IBM i PEM

```
pem.private = /dir/keystore_file_private_key
pem.public = /dir/keystore_file_public_keys
pem.password = password
V 9.2.2 pem.encrypted = no
```

Java JKS

```
jks.keystore = dir/Keystore
jks.certificate = certificate_label
jks.encrypted = no
jks.keystore_pass = password
jks.key_pass = password
jks.provider = IBMJCE
```

Java JCEKS

```
jceks.keystore = dir/Keystore
jceks.certificate = certificate_label
jceks.encrypted = no
jceks.keystore_pass = password
jceks.key_pass = password
jceks.provider = IBMJCE
```

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 102. Souhrn parametrů potřebných pro každý typ konfiguračního souboru

Parametry	Povinné	Typ konfiguračního souboru				
		Java (PKCS#11, JKS, JCEKS a JCERACFKS)	**IBM i PEM**	**PKCS#11**	**cms**	**AMSCRED**
keystore	✓	✓			✓	

Tabulka 102. Souhrn parametrů potřebných pro každý typ konfiguračního souboru (pokračování)						
		Typ konfiguračního souboru				
Parametry	**Povinné**	**Java (PKCS#11, JKS, JCEKS a JCERACFKS)**	IBM i **PEM**	**PKCS#11**	**cms**	**AMSCRED**
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`		✓	V 9.2.2 IBM i ✓	V 9.2.2 ✓		
`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 9.2.2 Toto pole byste měli chránit pomocí nativního nástroje pro ochranu heslem AMS ; viz “Ochrana hesel” na stránce 629

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.

V 9.2.0 V 9.2.0 Pouze pro operace Java ; toto pole byste měli chránit pomocí nástroje pro ochranu hesla produktu Java AMS ; viz “Ochrana hesel” na stránce 629.

V 9.2.2 Pouze pro nativní operace; toto pole byste měli chránit pomocí nativního nástroje pro ochranu hesla AMS ; viz “Ochrana hesel” na stránce 629.

secondary_keystore
PKCS#11 pouze.

Název cesty úložiště klíčů CMS 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 629.

encrypted

V 9.2.0 V 9.2.0 Java pouze konfigurace.

V 9.2.2 Pouze konfigurace Java, PKCS#11a IBM i PEM .

Stav hesla.

keystore_pass

Pouze konfigurace Java .

Heslo pro soubor úložiště klíčů.

V 9.2.0 V 9.2.0 Pouze pro operace Java . Toto pole byste měli chránit pomocí nástroje pro ochranu hesla produktu Java AMS ; viz “Ochrana hesel” na stránce 629.

key_pass

Pouze konfigurace Java .

Heslo pro soukromý klíč uživatele.

V 9.2.0 V 9.2.0 Pouze pro operace Java ; toto pole byste měli chránit pomocí nástroje pro ochranu hesla produktu Java AMS ; viz “Ochrana hesel” na stránce 629.

V 9.2.0 V 9.2.0 **keyfile**

Poskytuje umístění počátečního klíče, který se má použít při ochraně nebo dešifrování hesel obsažených v tomto konfiguračním souboru; viz “Ochrana hesel” na stránce 629

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

V 9.2.0 V 9.2.0

Měli byste chránit hesla a další citlivé informace obsažené v souboru `keystore.conf` . Další informace viz **runamscred** .

Příklad souboru `keystore.conf` :

V 9.2.0 V 9.2.0

```
# 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 643
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 pro non-IBM JRE s AMS

Operace IBM MQ classes for Java a IBM MQ classes for JMS podporují operaci Advanced Message Security při spuštění s prostředím JRE jiným nežIBM .

Advanced Message Security (AMS) implementuje Syntax Message Syntax (CMS). Syntaxe CMS se používá k digitálnímu podpisu, shrnutí, ověření nebo šifrování libovolného obsahu zprávy.

Z produktu IBM MQ 9.0podpora Advanced Message Security v produktu IBM MQ classes for Java a IBM MQ classes for JMS používá pro podporu systému CMS otevřený zdrojový balík Bouncy Castle . To znamená, že tyto třídy mohou podporovat operaci Advanced Message Security při spouštění s jinými nežIBM JRE.

Před produktem IBM MQ 9.0nebyl produkt Advanced Message Security podporován v jiných prostředích JRE nežIBM v klientech Java . Podpora produktu Advanced Message Security v produktu IBM MQ classes for Java a IBM MQ classes for JMS závisí na podpoře CMS, která je konkrétně poskytována implementací rozšíření JCE (Java Cryptography Extensions) produktu IBM . Kvůli tomuto omezení byla funkce k dispozici pouze při použití prostředí Java runtime environment (JRE), které obsahovalo poskytovatele JCE Java .

Číslování lokalit a verzí pro soubory JAR objektu Bouncy Castle

Soubory JAR Bouncy Castle, které jsou potřebné pro podporu prostředí JRE jiných nežIBM , jsou zahrnuty jako součást instalačního balíku produktu IBM MQ classes for Java a IBM MQ classes for JMS .

Použité soubory JAR Bouncy Castle jsou tyto soubory:

Soubor JAR poskytovatele, který má zásadní význam pro operace Bouncy Castle.
Tento soubor JAR se nazývá `bcprov-jdk15on.jar`.

Soubor JAR "PKIX", který obsahuje podporu pro operace CMS, které používá produkt Advanced Message Security.
Tento soubor JAR se nazývá `bcpkix-jdk15on.jar`.

V 9.2.0.4 V 9.2.4 **Soubor JAR "util", který obsahuje třídy používané jinými soubory JAR Bouncy Castle.**
Tento soubor JAR se nazývá `bcutil-jdk15on.jar`.

Závislosti

Třídy IBM MQ 9.1 a novější byly testovány s prostředím JRE produktu IBM a JRE Oracle . Je pravděpodobné, že se úspěšně spustí pod libovolným J2SE-compliant JRE. Měli byste však vzít na vědomí následující závislosti:

- Nejsou žádné změny v konfiguraci produktu Advanced Message Security .
- Třídy Hrad Bouncy 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 poskytovanou prostředím JRE.

  Důležité: Z tohoto důvodu musí použité prostředí JRE obsahovat implementaci poskytovatele JCE.
- Chcete-li použít některé *silné* šifrovací algoritmy, budete možná muset nainstalovat soubory zásad *unrestricted* pro implementaci JCE JRE.

  Další podrobnosti naleznete v dokumentaci k prostředí JRE.
- Pokud jste povolili zabezpečení produktu Java :
  - Přidejte `java.security.SecurityPermissioninsertProvider.BC` do aplikace tak, aby třídy Bouncy Castle mohly být použity jako poskytovatel zabezpečení.
  - Udělte prostor `java.security.AllPermission` souborům JAR Bouncy Castle, které jsou:

    V 9.2.0.4 V 9.2.4 *mq_install_dir*`/java/lib/bcutil-jdk15on.jar`
    mq_install_dir`/java/lib/bcpkix-jdk15on.jar`

mq_install_dir/java/lib/bcprov-jdk15on.jar

Související pojmy

Co je nainstalováno pro třídy IBM MQ pro JMS

Co je nainstalováno pro třídy IBM MQ pro jazyk Java

Multi Vyjimky agenta MCA (Message Channel Agent) a AMS

Interception MCA umožňuje správci front spuštěnému v rámci produktu IBM MQ selektivně povolit použití zásad pro kanály připojení serveru.

Interception MCA umožňuje klientům, kteří zůstanou mimo produkt AMS , stále být připojeni ke správci front, a jejich zprávy budou šifrovány a dešifrovány.

Funkce MCA interception je určen k poskytnutí funkce AMS , pokud AMS nelze povolit na klientovi. Všimněte si, že použití zachycení agenta MCA a klienta s aktivovanou AMSmá za následek dvojí ochranu zpráv, které mohou být problematické pro příjem aplikací. Další informace viz “Zakázání produktu Advanced Message Security na straně klienta” na stránce 633.

Poznámka: Zachytávače MCA nejsou podporovány pro kanály AMQP nebo MQTT.

Konfigurační soubor úložiště klíčů

Při výchozím nastavení je konfigurační soubor úložiště klíčů pro zachycení agenta MCA `keystore.conf` a nachází se v adresáři `.mqs` v cestě k adresáři HOME uživatele, který spustil správce front nebo modul listener. Úložiště klíčů lze také konfigurovat pomocí proměnné prostředí MQS_KEYSTORE_CONF. Další informace o konfiguraci úložiště klíčů produktu AMS naleznete v tématu “Použití úložišť klíčů a certifikátů s produktem AMS” na stránce 624.

Chcete-li povolit zachycení agenta MCA, je třeba zadat název kanálu, který chcete použít v konfiguračním souboru úložiště klíčů. V případě zachycení agenta MCA lze použít pouze typ úložiště klíčů cms.

Příklad nastavení zachycení agenta MCA naleznete v tématu “Příklad příkazu MCA interception pro AMS” na stránce 631 .

Upozornění: Na vybraných kanálech musíte dokončit ověření a šifrování klienta, například pomocí SSL a SSLPEER nebo CHLAUTH TYPE (SSLPEERMAP), abyste zajistili, že se k této schopnosti budou moci připojit pouze autorizovaní klienti.

IBM i

Pokud váš podnik používá produkt IBM ia vy jste vybrali komerční certifikační autoritu (CA) k podepsání certifikátu, produkt Digital Certificate Manager vytvoří žádost o certifikát ve formátu PEM (Privacy-Enhanced Mail). Je třeba předat požadavek na zvolenou CA.

Chcete-li to provést, je třeba použít následující příkaz k výběru správného certifikátu pro kanál určený v produktu `channelname`:

```
pem.certificate.channel.channelname
```

Příklad příkazu MCA interception pro AMS

Příklad úlohy, jak nastavit zachycení agenta MCA AMS .

Než začnete

Upozornění: Na vybraných kanálech musíte dokončit ověření a šifrování klienta, například pomocí SSL a SSLPEER nebo CHLAUTH TYPE (SSLPEERMAP), abyste zajistili, že se k této schopnosti budou moci připojit pouze autorizovaní klienti.

Pokud váš podnik používá produkt IBM ia vy jste vybrali komerční certifikační autoritu (CA) k podepsání certifikátu, produkt Digital Certificate Manager vytvoří žádost o certifikát ve formátu PEM (Privacy-Enhanced Mail). Je třeba předat požadavek na zvolenou CA.

Informace o této úloze

Tato úloha vás provede procesem nastavení vašeho systému tak, aby používal zachycování zpráv MCA, a poté ověření nastavení.

Poznámka: Před verzí IBM WebSphere MQ 7.5byl produkt AMS přídavným produktem, který měl být instalován a zachytávač konfigurován pro ochranu aplikací. V produktu IBM WebSphere MQ 7.5jsou zachytávače automaticky zahrnuty a dynamicky povoleny v prostředí klienta a běhového prostředí klienta a serveru MQ . V tomto příkladu pro práci s produktem MCA jsou zachytávače poskytovány na konci kanálu serveru a v kroku 12 se používá starší běhové prostředí klienta (v kroku 12) k vložení nechráněných zpráv do kanálu tak, aby jej bylo možné považovat za ochranu zachytávačů MCA. Pokud by tento příklad použil klienta produktu IBM WebSphere MQ 7.5 nebo novější, způsobilo by to, že se zpráva bude chránit dvakrát, protože zachytávač běhového prostředí klienta MQ a zachytávač MCA by oba tyto zprávy při vstupu do produktu MQochránili.

Upozornění: Nahraďte `userID` v kódu vaším ID uživatele.

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 nemusí být nutné vytvořit certifikát pro bob.

```
INSTLOC=/opt/mq90
KEYSTORELOC=/home/testusr/ssl/ams1
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

gsk8capicmd_64 -keydb -create -db $KEYSTORELOC/alicekey.kdb -pw passw0rd -stash
gsk8capicmd_64 -keydb -create -db $KEYSTORELOC/bobkey.kdb -pw passw0rd -stash
gsk8capicmd_64 -cert -create -db $KEYSTORELOC/alicekey.kdb -pw passw0rd
-label alice_cert -dn "cn=alice,O=IBM,c=IN" -default_cert yes
gsk8capicmd_64 -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 dvěma klíčovými databázemi tak, aby každý uživatel mohl úspěšně identifikovat ostatní.

   Je důležité, abyste použili metodu popsanou v **Úloha 5. Sdílení certifikátů** v příručce **Quick Start Guide** (Windows nebo AIX and Linux).

3. Vytvořte `keystore.conf` s touto konfigurací: `Keystore.conf location: /home/userID/ssl/ams1/`

```
cms.keystore = /home/userID/ssl/ams1/alicekey
cms.certificate.channel.SYSTEM.DEF.SVRCONN = alice_cert
```

4. Vytvořit a spustit správce front `AMSQMGR1`
5. Definování modulu listener s parametrem *port* `14567` a *control* `QMGR`
6. Zakažte oprávnění kanálu nebo nastavte pravidla pro oprávnění kanálu.

   Další informace viz SET CHLAUTH .

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.
10. Nastavte zásady 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 konfiguraci kanálu:

```
export MQSERVER='SYSTEM.DEF.SVRCONN/TCP/127.0.0.1(14567)'
```

12. Spusťte produkt **amqsputc** z klienta MQ , který automaticky nepovoluje zachytávač MCA; například IBM WebSphere MQ 7.1 nebo dřívější klient. Vložte následující dvě zprávy:

```
/opt/mqm/samp/bin/amqsputc TESTQ TESTQMGR
```

13. Odeberte zásadu zabezpečení a ověřte výsledek:

```
setmqspl -m AMSQMGR1 -p TESTQ -remove
dspmqspl -m AMSQMGR1
```

14. Procházejte frontu z instalace produktu IBM MQ 9.0 :

```
/opt/mq90/samp/bin/amqsbcg TESTQ AMSQMGR1
```

Výstup procházení zobrazuje zprávy v šifrovaném formátu.

15. 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
```

16. Spusťte produkt **amqsgetc** z instalace produktu IBM MQ 9.0 :

```
/opt/mqm/samp/bin/amqsgetc TESTQ TESTQMGR
```

Související úlohy

“Stručná úvodní příručka pro AMS s klienty Java” na stránce 612
Pomocí této příručky můžete rychle nakonfigurovat produkt Advanced Message Security a poskytnout zabezpečení zpráv pro aplikace produktu Java , které se připojují pomocí vazeb klienta. Po dokončení tohoto procesu jste vytvořili úložiště klíčů k ověření identit uživatelů a definované zásady pro podepisování a šifrování pro správce front.

Související odkazy

“Známá omezení AMS” na stránce 584
Existuje celá řada IBM MQ voleb, které buď nejsou podporovány, nebo mají omezení pro Advanced Message Security.

Zakázání produktu Advanced Message Security na straně klienta

Pokud používáte klienta IBM WebSphere MQ 7.5 nebo novější k připojení ke správci front z dřívější verze produktu a je-li hlášena chyba 2085 (MQRC_UNKNOWN_OBJECT_NAME), je třeba vypnout produkt IBM MQ Advanced Message Security (AMS).

Informace o této úloze

V produktu IBM WebSphere MQ 7.5je produkt IBM MQ Advanced Message Security (AMS) automaticky aktivován v klientovi IBM MQ a při výchozím nastavení se klient pokusí zkontrolovat zásady zabezpečení pro objekty ve správci front. Nicméně servery ve starších verzích produktu, například IBM WebSphere MQ 7.1, nemají povoleny AMS a způsobí chybu 2085 (MQRC_UNKNOWN_OBJECT_NAME) chyby.

Je-li tato chyba hlášena při pokusu o připojení ke správci front ze starší verze produktu, můžete produkt AMS vypnout následujícím způsobem:

- Pro klienty produktu Java lze následujícími způsoby:

  - Nastavením proměnné prostředí AMQ_DISABLE_CLIENT_AMS.
  - Nastavením systémové vlastnosti Java na hodnotu com.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS.
  - Použitím vlastnosti DisableClientAMS, pod stanzou **Security** v souboru `mqclient.ini` .
- Pro klienty typu C platí jedním z následujících způsobů:
  - Nastavením proměnné prostředí MQS_DISABLE_ALL_INTERCEPT.
  - Použitím vlastnosti DisableClientAMS, pod stanzou **Security** v souboru `mqclient.ini` .

Poznámka: V produktu IBM WebSphere MQ 7.5můžete také použít proměnnou prostředí AMQ_DISABLE_CLIENT_AMS. pro klienty jazyka C. V produktu IBM MQ 8.0již nelze použít proměnnou prostředí AMQ_DISABLE_CLIENT_AMS pro klienty jazyka C. Namísto toho je třeba použít proměnnou prostředí MQS_DISABLE_ALL_INTERCEPT.

Procedura

- Chcete-li v klientu vypnout AMS , použijte jednu z následujících možností:

  proměnná prostředí AMQ_DISABLE_CLIENT_AMS
  Tuto proměnnou je třeba nastavit v následujících případech:
  - Používáte-li prostředí JRE (Java Runtime Environment) jiné než prostředí IBM Java Runtime Environment (JRE)
  - Používáte-li produkt IBM WebSphere MQ 7.5nebo novější IBM MQ classes for JMS nebo klienta IBM MQ classes for Java .

  Vytvořte proměnnou prostředí AMQ_DISABLE_CLIENT_AMS a nastavte ji na hodnotu TRUE v prostředí, v němž je aplikace spuštěna. Příklad:

  ```
  export AMQ_DISABLE_CLIENT_AMS=TRUE
  ```

  Vlastnost systému Java com.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS
  V případě 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` , když je vyvolán příkaz Java :

  ```
  java -Dcom.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS=TRUE -cp <MQ_INSTALLATION_PATH>/java/lib/
  com.ibm.mqjms.jar  my.java.applicationClass
  ```

  Případně můžete zadat systémovou vlastnost Java v rámci konfiguračního souboru JMS `jms.config`, pokud aplikace tento soubor používá.

  proměnná prostředí MQS_DISABLE_ALL_INTERCEPT
  Tuto proměnnou je třeba nastavit v případě, že používáte produkt IBM MQ 8.0 nebo novější s nativními klienty a v klientu je třeba zakázat produkt AMS .

  Vytvořte proměnnou prostředí MQS_DISABLE_ALL_INTERCEPT a nastavte ji na hodnotu TRUE v prostředí, v němž je klient spuštěn. Příklad:

  ```
  export MQS_DISABLE_ALL_INTERCEPT =TRUE
  ```

  Proměnnou prostředí MQS_DISABLE_ALL_INTERCEPT můžete použít pouze pro klienty jazyka C. Pro klienty produktu Java je třeba namísto 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 stanzou **Security** soubor `mqclient.ini` , jak ukazuje následující příklad:

  ```
  Security:
  DisableClientAMS=Yes
  ```

Můžete také povolit produkt AMS , jak ukazuje následující příklad:

```
Security:
DisableClientAMS=No
```

Jak pokračovat dále

Další informace o problémech při otevírání chráněných front produktu AMS naleznete v tématu Problémy při otevírání chráněných front při použití produktu AMS s produktem JMS.

Související pojmy

"Vyjimky agenta MCA (Message Channel Agent) a AMS" na stránce 631
Interception MCA umožňuje správci front spuštěnému v rámci produktu IBM MQ selektivně povolit použití zásad pro kanály připojení serveru.

Související úlohy

Konfigurace klienta pomocí konfiguračního souboru

Související odkazy

Konfigurační soubor IBM MQ classes for JMS

Požadavky na certifikát pro AMS

Certifikáty musí mít veřejný klíč RSA, aby jej bylo možné použít 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 43.

Rozšíření použití klíče

Rozšíření pro použití klíče umístí další omezení na způsob, jakým lze použít certifikát.

V produktu Advanced Message Securitymusí být klíčové využití certifikátů X.509 v3 nastaveno v souladu se specifikací RFC 5280.

Je-li pro kvalitu ochrany nastavena rozšíření použití certifikátů, musí tato sada obsahovat alespoň jednu z těchto dvou hodnot:

- **`nonRepudiation`**
- **`digitalSignature`**

Je-li nastavena rozšíření použití klíče certifikátu pro kvalitu ochrany utajení, musí tato sada obsahovat:

- **`keyEncipherment`**

Je-li sada použití rozšíření certifikátů nastavena na kvalitu ochrany utajení, musí tato sada obsahovat:

- **`dataEncipherment`**

Rozšířené použití klíče dále zpřesňuje 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 produktu AMS" na stránce 654
Advanced Message Security zásady ochrany dat znamenají kvalitu ochrany (QOP).

Metody ověření platnosti certifikátů v produktu AMS

Pomocí produktu Advanced Message Security můžete zjišťovat a odmítat odvolané certifikáty, takže zprávy ve vašich frontách nebudou 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 nakonfigurovat buď pro kontrolu OCSP, nebo pro kontrolu CRL, nebo obojí. Jsou-li povoleny obě metody, pak produkt AMS z důvodů výkonu nejprve použije OCSP pro stav odvolání jako první. Pokud je stav odvolání certifikátu neurčený po kontrole OCSP, produkt AMS použije kontrolu CRL.

Všimněte si, že při výchozím nastavení je povolena kontrola OCSP i CRL.

Související pojmy

"Protokol OCSP (Online Certificate Status Protocol) v produktu AMS" na stránce 636
Protokol OCSP (Online Certificate Status Protocol) určuje, zda byl certifikát odvolán, a proto pomáhá určit, zda může být certifikát důvěryhodný. Protokol OCSP je ve výchozím nastavení povolen.

"Seznamy odvolaných certifikátů (CRL) v produktu AMS" na stránce 638
Seznamy CRL obsahují seznam certifikátů, které byly označeny certifikační autoritou (CA), protože již nejsou důvěryhodné z různých důvodů, například soukromý klíč byl ztracen nebo ohrožen.

Protokol OCSP (Online Certificate Status Protocol) v produktu AMS

Protokol OCSP (Online Certificate Status Protocol) určuje, zda byl certifikát odvolán, a proto pomáhá určit, zda může být certifikát důvěryhodný. Protokol OCSP je ve výchozím nastavení povolen.

Protokol OCSP není v systémech IBM i sytems podporován.

Povolení kontroly OCSP v nativních zachytávačích produktu Advanced Message Security
Kontrola protokolu OCSP (Online Certificate Status Protocol) v produktu Advanced Message Security je standardně povolena na základě informací v použitých certifikátech.

Postup

Přidejte do konfiguračního souboru úložiště klíčů tyto volby:

Poznámka: Všechna stanza OCSP jsou volitelná a lze ji zadat nezávisle.

Volba	Popis
`ocsp.enable=off`	Povolte kontrolu protokolu OCSP, pokud má kontrolovaný certifikát přístup IIA (Authority Info Access) s přístupovou metodou PKIX_AD_OCSP obsahující identifikátor URI místa, kde se nachází odpovídací modul OCSP. Možné hodnoty: on nebo `off`.
`ocsp.url=`*`responder_URL`*	Adresa URL odpovídacího modulu OCSP. Je-li tato volba vynechána, je kontrola neAIXA protokolu OCSP zakázána.
`ocsp.http.proxy.host=`*`OCSP_proxy`*	Adresa URL serveru proxy OCSP. Je-li tato volba vynechána, nebude server proxy použit pro kontroly online certifikátů bez systému AIA.
`ocsp.http.proxy.port=`*`port_number`*	Číslo portu serveru proxy OCSP. Je-li tato volba vynechána, bude použit 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.

Volba	Popis
`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. Standardní 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, když server OCSP nemůže být dosažen během časového limitu. Možné hodnoty jsou: • `ACCEPT` Povoluje certifikát • `WARN` Povoluje certifikát a protokoluje varování • `REJECT` Zabraňuje použití certifikátu a protokoluje chybu

Povolení kontroly OCSP v produktu Java v produktu AMS
Chcete-li povolit kontrolu OCSP pro produkt Java v produktu Advanced Message Security, upravte soubor `java.security` nebo konfigurační soubor úložiště klíčů.

Informace o této úloze

V produktu Advanced Message Securitylze povolit kontrolu protokolu OCSP dvěma způsoby:

Použití souboru java.security
Zkontrolujte, zda váš certifikát obsahuje rozšíření certifikátu AIA (Authority Information Access).

Postup

1. Pokud AIA není nastavena nebo chcete 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 umožněte kontrolu OCSP upravením souboru `$JAVA_HOME/lib/security/java.security` následujícím řádkem:

   ```
   ocsp.enable=true
   ```

2. Je-li nastaveno AIA, povolte kontrolu OCSP upravením souboru `$JAVA_HOME/lib/security/java.security` následujícím řádkem:

   ```
   ocsp.enable=true
   ```

Jak pokračovat dále

Pokud používáte správce zabezpečení produktu Java , příliš dokončete konfiguraci, přidejte následující oprávnění produktu Java do produktu `lib/security/java.policy`

```
permission java.security.SecurityPermission "getProperty.ocsp.enable";
```

Použití souboru keystore.conf

Postup

Přidejte do konfiguračního souboru následující atribut:

```
ocsp.enable=true
```

Důležité: Nastavení tohoto atributu v konfiguračním souboru přepíše nastavení java.security .

Jak pokračovat dále

Chcete-li dokončit konfiguraci, přidejte následující oprávnění produktu Java do produktu `lib/security/java.policy`:

```
permission java.security.SecurityPermission "getProperty.ocsp.enable";
permission java.security.SecurityPermission "setProperty.ocsp.enable";
```

Seznamy odvolaných certifikátů (CRL) v produktu AMS

Seznamy CRL obsahují seznam certifikátů, které byly označeny certifikační autoritou (CA), protože již nejsou důvěryhodné 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 certifikačního řetězce certifikační autority (CA ' s) až po kotvu důvěryhodnosti. Kotva důvěryhodnosti je důvěryhodný soubor úložiště klíčů, který obsahuje důvěryhodný certifikát, nebo důvěryhodný kořenový certifikát, který se používá k deklarování důvěryhodnosti certifikátu. Produkt AMS ověřuje cestu certifikátu pomocí ověřovacího algoritmu PKIX. Když je řetěz vytvořen a ověřen, AMS dokončí ověření platnosti certifikátu, které zahrnuje ověření platnosti vydání a datum vypršení platnosti každého certifikátu v řetězci proti aktuálnímu datu, kontrolou, zda je rozšíření použití klíče přítomno v certifikátu koncové entity. Je-li rozšíření připojeno k certifikátu, produkt AMS ověří, zda jsou nastaveny také položky **digitalSignature** nebo **nonRepudiation** . Pokud nejsou, je `MQRC_SECURITY_ERROR` ohlášen a zaprotokolován. Produkt AMS dále stahuje seznamy CRL ze souborů nebo z LDAP v závislosti na tom, jaké hodnoty byly zadány v konfiguračním souboru. AMSpodporuje pouze seznamy CRL, které jsou kódovány ve formátu DER. Není-li v konfiguračním souboru úložiště klíčů nalezena žádná konfigurace CRL, AMS neprovede žádnou kontrolu platnosti CRL. Pro každý certifikát CA AMS dotazuje LDAP na CRL pomocí rozlišujících názvů CA pro vyhledání svého seznamu CRL. Do dotazu LDAP jsou zahrnuty následující atributy:

```
certificateRevocationList,
certificateRevocationList;binary,
authorityRevocationList,
authorityRevocationList;binary
deltaRevocationList
deltaRevocationList;binary,
```

Poznámka: Produkt `deltaRevocationList` je podporován pouze v případě, že je určen jako distribuční body.

Povolení ověření platnosti certifikátu a podpory seznamu odvolaných certifikátů v nativních zachytávačích

Je třeba upravit konfigurační soubor úložiště klíčů tak, aby produkt Advanced Message Security mohl stáhnout soubory CLR ze serveru LDAP (Lightweight Directory Access Protocol).

Informace o této úloze

IBM i Povolení ověření platnosti certifikátu a podpora seznamu odvolaných certifikátů v nativních zachytávačích není podporováno pro produkt Advanced Message Security v systému IBM i.

Postup

Přidejte do konfiguračního souboru následující volby:

Poznámka: Všechna stanza CRL jsou volitelná a mohou být uvedena 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. Více hostitelů LDAP se používá k zajištění transparentního překonání selhání v případě selhání připojení LDAP. Očekává se, že všechny servery LDAP jsou repliky a obsahují stejná data. Když se zachytávač AMS Java úspěšně připojí k serveru LDAP, nedojde k pokusu o stažení seznamů CRL ze zbývajících serverů.
`crl.cdp=off`	Použijte tuto volbu ke kontrole nebo použití rozšíření CRLDistributionPoints v certifikátech.
`crl.ldap.version=3`	Číslo verze protokolu LDAP. Možné hodnoty: 2 nebo 3.
`crl.ldap.user=cn=`*`username`*	Přihlaste se k serveru LDAP. Není-li tato hodnota zadána, musí být atributy CRL v LDAP musejí být čitelné pro celý svět.
`crl.ldap.pass=`*`password`*	Heslo pro server LDAP.
V 9.2.2 `crl.ldap.encrypted=`*`no/yes`*	Zda je server `clr.ldap.pass` šifrovaný či nikoli. Další informace najdete v tématu Ochrana hesel v konfiguračních souborech AMS .
`crl.ldap.cache_lifetime=0`	Životnost mezipaměti LDAP v sekundách. Možné hodnoty: 0-86400.
`crl.ldap.cache_size=50`	Velikost mezipaměti LDAP. Tuto volbu lze zadat pouze v případě, že je hodnota `crl.ldap.cache_lifetime` větší než hodnota `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 sadou GSKit.
`crl.http.timeout=30`	Doba čekání na odpověď serveru, v sekundách, po které AMS vyprší časový limit.
`crl.http.cache_size=0`	Velikost mezipaměti HTTP, v bajtech.

Volba	Popis
`crl.unknown=ACCEPT`	Definuje chování, pokud nelze v rámci časového limitu dosáhnout serveru CRL. Možné hodnoty jsou: • ACCEPT Povoluje certifikát • WARN Povoluje certifikát a protokoluje varování • REJECT Zabraňuje použití certifikátu a protokoluje chybu

Povolení podpory seznamu odvolaných certifikátů v produktu Java v produktu AMS
Chcete-li v produktu Advanced Message Securitypovolit podporu CRL, je třeba upravit konfigurační soubor úložiště klíčů tak, aby produkt AMS mohl stahovat seznamy CRL ze serveru LDAP (Lightweight Directory Access Protocol) a konfigurovat soubor java.security .

Postup

1. Přidejte do konfiguračního souboru následující volby:

Header	Popis
`crl.ldap.host=`*`host_name`*	Název hostitele LDAP.
`crl.ldap.port=`*`port_number`*	Číslo portu serveru LDAP. Můžete uvést až 11 serverů. Více hostitelů LDAP se používá k zajištění transparentního překonání selhání v případě selhání připojení LDAP. Očekává se, že všechny servery LDAP jsou repliky a obsahují stejná data. Když se zachytávač AMS Java úspěšně připojí k serveru LDAP, nedojde k pokusu o stažení seznamů CRL ze zbývajících serverů. Produkt Java nepoužívá hodnoty `crl.ldap.user` a crl.ldaworldp.pass . Nepoužívá při připojování k serveru LDAP uživatele a heslo. V důsledku toho musí být atributy CRL v LDAP na světě čitelné.
`crl.cdp=on/off`	Použijte tuto volbu ke kontrole nebo použití rozšíření CRLDistributionPoints v certifikátech.

2. Upravte soubor `JRE/lib/security/java.security` s následujícími vlastnostmi:

Název vlastnosti	Popis
`com.ibm.security.enableCRLDP`	Tato vlastnost má následující hodnoty: `true`, `false`. Je-li při provádění kontroly odvolání certifikátu nastavena hodnota `true`, jsou seznamy CRL umístěny s použitím adresy URL z rozšíření certifikátu CRL rozšíření certifikátu. Je-li nastaven na hodnotu `false` nebo není nastaven, kontrola seznamu CRL pomocí rozšíření distribučních bodů CRL je zakázána.

Název vlastnosti	Popis
`ibm.security.certpath.ldap.cache.lifetime`	Tuto vlastnost lze použít k nastavení životnosti položek v mezipaměti paměti protokolu LDAP CertStore na hodnotu v sekundách. Hodnota 0 zakáže mezipaměť; -1 znamená neomezenou životnost. Pokud není nastaven, výchozí životnost je 30 sekund.
`com.ibm.security.enableAIAEXT`	Tato vlastnost má následující hodnoty: `true`, `false`. Je-li nastaven na hodnotu `true`, prověřuje se každá rozšíření přístupu k informacím o oprávnění, která se nacházejí v certifikátech použité cesty k certifikátu, aby určily, zda obsahují identifikátory URI LDAP. Pro každý nalezený identifikátor URI LDAP je vytvořen objekt LDAPCertStore a přidán do kolekce CertStores , který se používá k vyhledání dalších certifikátů, které jsou vyžadovány pro sestavení cesty k certifikátu. Je-li tento parametr nastaven na hodnotu `false` nebo není nastaven, nebudou vytvořeny další objekty LDAPCertStore .

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 potvrdí certifikáty příjemce, když jsou zprávy vloženy do fronty chráněné soukromí, a ověřovat certifikáty odesílatele, když jsou zprávy načítány z chráněné fronty (integrita nebo soukromí). Validace v tomto případě zahrnuje ověření, že příslušné certifikáty nejsou registrovány v příslušném seznamu CRL.

Produkt Advanced Message Security používá služby zabezpečení SSL systému IBM k ověření platnosti certifikátů odesilatele a příjemce. Podrobnou dokumentaci týkající se ověření certifikátu Systému SSL lze nalézt v příručce z/OS Cryptographic Services System Secure Sockets Layer Programming (SC24-5901).

Chcete-li povolit kontrolu CRL, určete umístění konfiguračního souboru CRL prostřednictvím definice CRLFILE DD v kódu JCL spuštěných úloh pro adresní prostor AMS. Ukázkový konfigurační soubor CRL, který lze upravit, je poskytnut v *thlqual*.SCSQPROC (CSQ40CRL). Nastavení povolená v tomto souboru jsou následující:

Tabulka 103. Advanced Message Security Konfigurační proměnné CRL

Proměnná	Platné hodnoty	Popis
crl.ldap.host[.n]	*název hostitele-nebo-název hostitele: port*	Ipaddr/název hostitele vašeho serveru LDAP, který hostí seznamy CRL vašich certifikátů vydavatele. Pokud pro váš server LDAP nezadáte číslo portu, použije se číslo portu určené parametrem crl.ldap.port .
crl.ldap.port	*port*	Číslo portu TCP/IP vašeho serveru LDAP.

Tabulka 103. Advanced Message Security Konfigurační proměnné CRL (pokračování)		
Proměnná	**Platné hodnoty**	**Popis**
crl.ldap.user	*uživatel_ldap*	Jméno uživatele LDAP, které má být použito pro připojení k serveru LDAP.
crl.ldap.pass	*heslo_ldap*	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 nezadáte číslo portu pro servery LDAP, použije se číslo portu určené parametrem crl.ldap.port . Každý server LDAP musí používat stejnou kombinaci crl.ldap.user/ password pro přístup.

Když je během inicializace adresního prostoru Advanced Message Security určena konfigurace CRLFILE DD a je povolena kontrola CRL, je konfigurace načtena. Není-li parametr CRLFILE DD zadán, nebo je-li konfigurační soubor CRL nedostupný nebo neplatný, je kontrola CRL zakázána.

Produkt AMS provádí kontrolu CRL pomocí služeb ověřování certifikátu SSL systému IBM následujícím způsobem:

Tabulka 104. Advanced Message Security Kontroly CRL		
Operace	**Kvalita ochrany**	**Ověřil certifikát**
PUT	Ochrana soukromí	Příjemce (i)
GET	Integrita/soukromí	Odesilatel

Pokud operace zprávy selže při kontrole seznamu CRL, provede příkaz Advanced Message Security následující akce:

Tabulka 105. Advanced Message Security Chování selhání kontroly CRL	
Operace	**Selhání kontroly CRL**
PUT	Zpráva se nevloží do cílové fronty. Kód dokončení operace MQCC_FAILED a kód příčiny MQRC_SECURITY_ERROR je vrácen do aplikace.
GET	Zpráva se odstraní z cílové fronty a přesune se do fronty chyb ochrany systému. Kód dokončení operace MQCC_FAILED a kód příčiny MQRC_SECURITY_ERROR je vrácen do aplikace.

AMS pro z/OS používá IBM Systémové služby SSL k ověření certifikátů, které zahrnuje CRL a kontrolu důvěryhodnosti. IBM System SSL poskytuje proměnnou prostředí GSK_CRL_SECURITY_LEVEL pro střední provoz kontroly CRL. Příklad:

```
GSK_CRL_SECURITY_LEVEL=MEDIUM
```

Tato proměnná je dokumentována v příručce z/OS Cryptographic Services System Secure Sockets Layer Programming. Mezi platná přiřazení patří:

- LOW-Ověření platnosti certifikátu selže, pokud nelze kontaktovat server LDAP.

- MEDIUM-Ověření platnosti certifikátu vyžaduje, aby byl server LDAP stykatelný, ale nevyžaduje definování seznamu CRL.
- HIGH-Ověření platnosti certifikátu vyžaduje, aby byl server LDAP contactable a seznam CRL, který má být definován.

Výchozí hodnota zabezpečení SSL systému IBM je hodnota MEDIUM. Tuto proměnnou můžete nastavit v konfiguračním souboru určeném prostřednictvím definice ENVARS DD v kódu JCL spuštěných úloh pro adresní prostor AMS. Ukázkový konfigurační soubor proměnné prostředí je poskytnut v souboru *thlqual*.SCSQPROC (CSQ40ENV).

Poznámka: Povinností správců je zajistit, aby příslušné služby LDAP byly k dispozici a udržovat záznamy CRL pro příslušné certifikační autority.

V 9.2.0 V 9.2.0 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 9.2.2 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 k zašifrování hesel uvnitř souboru, který je přístupný pro uživatele chránící `keystore.conf` soubor.

   V 9.2.2 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 v systému z/OS

Informace o této úloze

Produkt Advanced Message Security implementuje tři úrovně ochrany: integritu, utajení a soukromí.

Se zásadou integrity se zprávy podepisují pomocí soukromého klíče původce (aplikace provádí operaci MQPUT). Integrita poskytuje detekci změny zprávy, ale samotný text zprávy není šifrován.

Při použití zásady ochrany důvěrných informací je zpráva při vložení do fronty šifrována. Tato zpráva je šifrována pomocí symetrického klíče a algoritmu určeného v příslušné zásadě Advanced Message Security . Samotný symetrický klíč je šifrován s veřejným klíčem každého příjemce (aplikace provádí MQGET). Veřejné klíče jsou přidruženy k certifikátům uloženým v klíčových kruzích.

Při použití zásady ochrany osobních údajů jsou zprávy podepisovány i šifrovány.

Je-li zpráva, která je chráněna soukromě, zařazena do fronty přijímající aplikací provádějící příkaz MQGET, musí být tato zpráva dešifrována. Protože byl zašifrován pomocí veřejného klíče příjemce, musí být dešifrován pomocí soukromého klíče příjemce, který se nachází v klíči svazku klíčů.

z/OS *Použití svazků klíčů SAF s produktem AMS v systému z/OS*

Produkt Advanced Message Security (AMS) využívá služby svazku klíčů SAF produktu z/OS k definování a správě certifikátů potřebných pro podepisování a šifrování. Produkty zabezpečení, které jsou funkčně ekvivalentní produktu RACF , lze použít namísto produktu RACF , pokud poskytují stejnou úroveň podpory.

Efektivní využití svazků klíčů může snížit správu potřebnou ke správě certifikátů.

Po vygenerování certifikátu (nebo při importu) musí být tento certifikát připojen ke klíči, který má být přístupný. Stejný certifikát může být připojen k více než jednomu svazku klíčů.

Produkt Advanced Message Security používá dvě sady svazků klíčů. Jedna sada se skládá z klíčových řetězců vlastněných jednotlivými ID uživatele, které pocházejí 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 chráněné integrity nebo pro utajení chráněné soukromí. Používá se také k dešifrování zpráv z chráněných chráněných dat nebo chráněných utajení při příjmu zpráv.

Druhá sada je jediným klíčovým svazkem vlastněným uživatelem adresního prostoru AMS . Obsahuje řetězec podpisových certifikátů CA potřebných k ověření certifikátů původce zprávy a příjemců.

Je-li použita ochrana soukromí nebo důvěrnosti, svazek klíčů vlastněný uživatelem adresního prostoru AMS také obsahuje certifikáty příjemců zprávy. 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, je soukromý klíč příslušných příjemců použit k dešifrování symetrického klíče, který je poté použit k dešifrování dat zprávy.

Produkt Advanced Message Security používá při hledání certifikátů a soukromých klíčů název svazku klíčů **drq.ams.keyring** . To platí jak pro uživatele, tak pro AMS -řetězce adresního prostoru adresního prostoru.

Pro ilustraci a další vysvětlení certifikátů a svazku klíčů a jejich role v ochraně dat viz Souhrn operací souvisejících s certifikátem.

Soukromý klíč používaný pro podepisování a dešifrování může mít libovolný popisek, ale musí být připojen 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 *Autorizace přístupu k příkazu RACDCERT pro produkt AMS v systému z/OS*

Oprávnění k použití příkazu RACDCERT je poinstalační úlohou, která měla být dokončena vaším systémovým programátorem produktu z/OS . Tato úloha zahrnuje udělení příslušných oprávnění administrátorovi zabezpečení produktu Advanced Message Security .

Jako souhrn jsou tyto příkazy potřebné k 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 příkladě uvádí *admin* ID uživatele vašeho administrátora zabezpečení nebo libovolného uživatele, kterého chcete použít, příkaz RACDCERT.

z/OS *Vytvoření certifikátů a svazků klíčů pro uživatele produktu AMS v systému z/OS*

This section documents the steps required to create the certificates and key rings necessary for z/OS users of Advanced Message Security (AMS), using a RACF Certificate Authority (CA).

Řešení problémů s certifikáty při použití produktu Advanced Message Security v systému z/OS

Máte-li problémy s certifikáty a chybějící položky v úložištích klíčů, můžete povolit trasování GSKIT.

V souboru, na který odkazuje definice ENVARS DD v rámci procedury spuštěné úlohy AMS , přidejte:

```
GSK_TRACE_FILE=/u/... /gsktrace
GSK_TRACE=0xff
```

Další informace naleznete v tématu Proměnné prostředí .

Pro každý přístup k úložišti klíčů jsou data zapsána do trasovacího souboru uvedeného v souboru GSK_TRACE_FILE.

Chcete-li formátovat trasovací soubor, použijte příkaz:

```
gsktrace inputtrace file > output_file
```

Scénář

Scénář odesílající aplikace a přijímající aplikace se používá k vysvětlení požadovaných kroků.

V následujících příkladech je user1 původce zprávy a user2 je příjemcem. ID uživatele adresního prostoru Advanced Message Security je WMQAMSD.

Všechny příkazy v příkladech, které jsou zde zobrazeny, jsou vydány z volby ISPF 6 administrativním ID uživatele admin.

z/OS *Definování certifikátu lokálního vydavatele certifikátů pro AMS v systému z/OS*

Používáte-li jako svého CA RACF , musíte vytvořit certifikát certifikační autority, pokud jste tak dosud neučinili. Zobrazený příkaz vytvoří certifikát certifikační autority (nebo podepisujícího subjektu). Tento příklad vytvoří certifikát s názvem AMSCA, který se použije při vytváření následných certifikátů, které budou odrážet identitu uživatelů a aplikací produktu Advanced Message Security .

Tento příkaz lze upravit, konkrétně SUBJECTSDN, aby odrážel strukturu pojmenování a konvence použité při instalaci:

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('AMSCA') O('ibm') C('us'))
KEYUSAGE(CERTSIGN) WITHLABEL('AMSCA')
```

Poznámka: Certifikáty podepsané s tímto certifikátem lokálního vydavatele certifikátů ukazují vydavatele CN=AMSCA, O=ibm, C=us, je-li uveden v seznamu s příkazem RACDCERT LIST.

z/OS *Vytvoření digitálního certifikátu se soukromým klíčem pro AMS v systému z/OS*

Pro každého uživatele produktu Advanced Message Security musí být vygenerován digitální certifikát se soukromým klíčem. V uvedeném příkladu jsou příkazy RACDCERT použity ke generování certifikátů pro uživatele user1 a user2, které jsou podepsány pomocí certifikátu lokálního CA identifikovaného 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
```

Příkaz RACDCERT ALTER je požadován pro přidání atributu TRUST do certifikátu. Když je certifikát poprvé vytvořen pomocí této procedury, má odlišný platný rozsah dat než podpisový certifikát. V důsledku toho jej produkt RACF označí jako NOTRUST, což znamená, že se certifikát nemá používat. Použijte příkaz RACDCERT ALTER k nastavení atributu TRUST.

Atributy KEYUSAGE HANDSHAKE, DATAENCRYPT a DOCSIGN musí být zadány pro certifikáty používané produktem Advanced Message Security.

Tabulka 106. RACDCERT KEYUSAGE hodnoty a indikátory

Hodnota KEYUSAGE	**Sada indikátorů**
navázání komunikace	digitalSignature a keyEncipherment
ŠIFROVÁNÍ DAT	dataEncipherment
DOCEDENÍ	nonRepudiation
CERTSIGN	keyCertZnaménko a cRLSign

z/OS *Vytvoření svazků klíčů RACF pro AMS v systému z/OS*

Zde uvedené příkazy vytvářejí svazek klíčů pro uživatele s definovanými uživateli produktu RACF user1, user2a uživatele úlohy adresního prostoru Advanced Message Security WMQAMSD. Název svazku klíčů je pevně stanoven Advanced Message Security a musí být zakódován, jak je zobrazeno, 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 k klíčům klíčů pro AMS v systému z/OS*

Připojte certifikáty uživatele a CA k prstenům klíčů:

```
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))
```

Certifikát obsahující soukromý klíč použitý k dešifrování musí být připojen k souboru svazku klíčů uživatele jako výchozí certifikát.

Atribut RACDCERT USAGE (SITE) zabraňuje v přístupu k soukromému klíči v klíčovém kruhu, zatímco atribut USAGE RACDCERT (OSOBNÍ) umožňuje použít soukromý klíč, pokud existuje. Certifikát User2musí být připojen k souboru svazku klíčů adresního prostoru Advanced Message Security , protože jeho veřejný klíč je nutný k zašifrování zpráv, které jsou vloženy do fronty. USAGE (SITE) omezuje riziko soukromého klíče uživatele user2.

Certifikát CERTAUTH s označením AMSCA musí být připojen ke svazku klíčů adresního prostoru Advanced Message Security , protože byl použit k podepsání certifikátu uživatele user1, který je původcem zprávy. Používá se k ověření podpisového certifikátu uživatele user1.

z/OS *Ověření klíčového řetězce pro AMS v systému z/OS*

Klíčový kroužek 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 ukazuje 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<:
```

Chcete-li zlepšit výkon, obsah souboru drq.ams.keyring přidružený k adresnímu prostoru AMS je uložen do mezipaměti pro životnost adresního prostoru. Změny na tomto svazku klíčů se nestanou účinnými automaticky. Administrátor může aktualizovat mezipaměť buď:

- Zastavení a restartování správce front.
- Pomocí příkazu z/OS MODIFY:

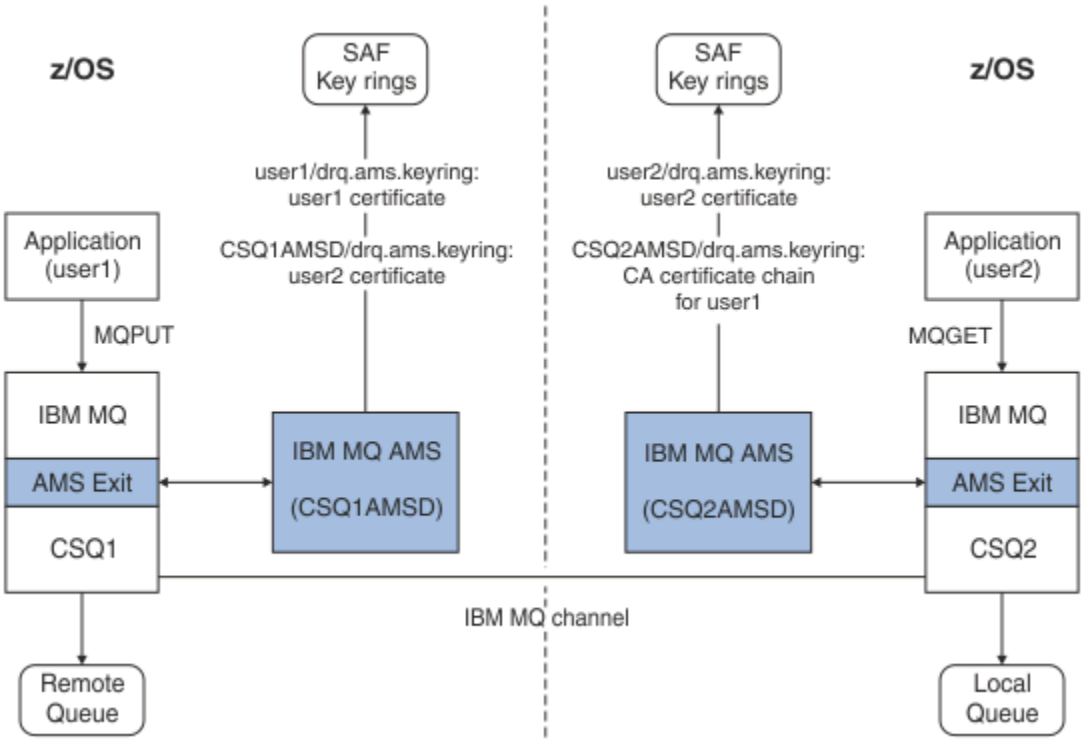
```
F qmgrAMSM,REFRESH KEYRING
```

Související úlohy

Provoz Advanced Message Security

z/OS *Souhrn operací souvisejících s certifikátem pro AMS v systému z/OS*

Obrázek 35 na stránce 648 ilustruje vztahy mezi odesíláním a přijímáním aplikací a příslušnými certifikáty. Scénář ilustruje použití vzdálených front mezi dvěma správci front produktu z/OS pomocí zásady ochrany soukromí pro ochranu dat. V produktu Obrázek 35 na stránce 648označuje "AMS". " Advanced Message Security".



Obrázek 35. Vztahy aplikací a certifikátů

V tomto diagramu aplikace spuštěná jako 'user1' vkládá 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 Advanced Message Security zásadu ochrany soukromí, což znamená, že zpráva je podepsaná i zašifrovaná.

Advanced Message Security zachytává zprávu při vložení a používá certifikát user2(uložený v souboru svazku klíčů adresního prostoru AMS) k šifrování symetrického klíče použitého k šifrování dat zprávy.

Všimněte si, že certifikát uživatele user2je připojen k svazku klíčů adresního prostoru AMS s volbou USAGE (SITE). To znamená, že uživatel adresního prostoru AMS má přístup k certifikátu a veřejnému klíči, ale ne k soukromému klíči.

Na přijímajícím konci Advanced Message Security zachycuje vydání user2a používá certifikát user2k dešifrování symetrického klíče, aby mohl dešifrovat data zprávy. Poté ověří podpis uživatele user1pomocí řetězce certifikátu CA uživatele user1uloženého v klíčovém kruhu uživatele adresního prostoru AMS.

S ohledem na tento scénář, ale s politikou ochrany dat integrity, by certifikáty pro uživatele user2 nebyly požadovány.

Chcete-li použít produkt Advanced Message Security k zařazení zpráv do front chráněných pomocí produktu IBM MQ, které mají zásady ochrany soukromí nebo integrity, Advanced Message Security musí mít přístup k těmto datovým položkám:

- Certifikát X.509 V2 nebo V3 a soukromý klíč pro uživatele zařazování zprávy do fronty.
- Řetěz certifikátů používaný k podepisování digitálních certifikátů všech zpráv podepisujících subjekty.
- Je-li zásada ochrany dat soukromá, jsou příjemci X.509 V2 nebo V3 určeným příjemcům. Zamýšlený příjemci jsou uvedeni v zásadě Advanced Message Security přidružené k frontě.

Pro procesy a aplikace spuštěné v produktu z/OSmusí produkt Advanced Message Security obsahovat certifikáty na dvou místech:

- Ve svazku klíčů spravovaného SAF přidružený k identitě RACF odesílající aplikace (aplikace, která zařazuje chráněnou zprávu) nebo přijímající aplikaci (pokud se používá ochrana soukromí).

  Certifikát, který produkt Advanced Message Security vyhledá, je výchozím certifikátem a musí obsahovat soukromý klíč. Advanced Message Security předpokládá uživatelskou identitu z/OS odesílající aplikace. To znamená, že se chová jako náhrada, takže má přístup k soukromému klíči uživatele.
- Ve svazku klíčů SAF přidruženém k uživateli adresního prostoru AMS.

  Při odesílání zpráv chráněných soukromě tento svazek klíčů obsahuje certifikáty veřejných klíčů příjemců zprávy. Při příjmu zpráv obsahuje řetězec certifikátů certifikačních autorit potřebných k ověření podpisu odesílatele zprávy.

Dřívější příklady použití RACF jako lokálního vydavatele certifikátů (CA). V instalaci však můžete použít jiného poskytovatele PKI (Certificate Authority). 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 , které pocházejí ze zpráv produktu IBM MQ chráněných produktem Advanced Message Security.

Jako mechanizmus pro generování požadavků na certifikáty můžete použít příkaz RACF RACDCERT, který může být exportován a odeslán poskytovateli PKI vaší volby, který má být vydán.

Zde je uveden souhrn kroků souvisejících s certifikátem:

1. Vyžádejte si vytvoření certifikátu CA, v němž RACF je lokální CA. Tento krok vynechte, pokud používáte jiného poskytovatele PKI.
2. Generovat uživatelské certifikáty podepsané CA.
3. Vytvořte svazky klíčů pro uživatele a ID adresního prostoru Advanced Message Security AMS.
4. Připojte certifikát uživatele k souboru svazku klíčů uživatele s výchozím atributem.
5. Připojte certifikáty příjemců do uživatelského svazku klíčů adresního prostoru Advanced Message Security AMS pomocí atributu použití (organizační jednotka) (Tento krok je nezbytný pouze pro uživatelské certifikáty, které budou nakonec příjemci zpráv chráněných soukromě).

6. Připojte řetězy certifikátů CA pro odesilatele zpráv do uživatelského svazku klíčů adresního prostoru Advanced Message Security AMS. (Tento krok je nezbytný pouze pro úlohy AMS, které budou ověřovat podpisy odesilatele.)

z/OS *Konfigurace infrastruktury PKI jiného produktu nežz/OS pro produkt AMS*

Advanced Message Security pro z/OS, používá X.509 V3 digitální certifikáty v ochranném zpracování zpráv umístěných nebo přijímaných z front produktu IBM MQ . Produkt Advanced Message Security sám 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 certifikát.

Je-li použit z/OS nebo není-z/OS používá-li PKI, AMS pro z/OS používá pouze klíčové kruhy, které jsou spravovány RACF nebo jeho ekvivalenty. Tyto svazky klíčů jsou založeny na prostředku SAF (Security Authorization Facility) a jsou úložištěm používaným produktem AMS for z/OS k získání certifikátů pro původce a příjemců zpráv umístěných nebo přijatých z front produktu 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 ve svazku klíčů spravovaného SAF, který je přidružen k ID uživatele z/OS původce zprávy.

Produkt RACF obsahuje schopnost importovat certifikáty a soukromé klíče do RACF-spravovaných svazků klíčů. Viz publikace z/OS Security Server RACF , kde jsou uvedeny podrobnosti a příklady toho, jak načíst certifikáty do spravovaných klíčů spravovaných klíčů produktu RACF .

Pokud vaše instalace používá jeden z podporovaných produktů PKI, prohlédněte si příručky, které jsou k produktu přiloženy, abyste získali informace o tom, jak ji nasadit.

Správa zásad zabezpečení produktu Advanced Message Security

Produkt Advanced Message Security používá zásady zabezpečení k určení šifrovacích šifrovacích algoritmů a podpisových algoritmů pro šifrování a ověřování zpráv, které procházejí přes fronty.

Přehled zásad zabezpečení pro produkt AMS

Zásady zabezpečení produktu Advanced Message Security jsou konceptuální objekty, které popisují způsob, jakým je zpráva šifrovaně šifrována a podepsána.

Podrobnosti o atributech zásad zabezpečení najdete v následujících dílčích tématech:

Související pojmy

“Kvalita ochrany v produktu AMS” na stránce 654
Advanced Message Security zásady ochrany dat znamenají kvalitu ochrany (QOP).

“Atributy zásady zabezpečení v produktu AMS” na stránce 653
Můžete použít produkt Advanced Message Security k výběru určitého algoritmu nebo metody k ochraně dat.

Názvy zásad v produktu AMS

Název zásady je jedinečný název, který identifikuje specifickou zásadu Advanced Message Security a frontu, na kterou se vztahuje.

Název zásady musí být stejný jako název fronty, na který se vztahuje. Mezi Advanced Message Security (AMS) existuje mapování jedna ku jedné. zásady a fronty.

Když vytvoříte zásadu se stejným názvem jako fronta, aktivujete zásadu pro tuto frontu. Fronty bez odpovídajících názvů zásad nejsou chráněny produktem AMS.

Rozsah zásady je relevantní pro lokálního správce front a jeho front. Vzdálení správci front musí mít své vlastní lokálně definované zásady pro fronty, které spravují.

Algoritmus podpisu v produktu AMS

Algoritmus podpisu označuje algoritmus, který se má použít při podepisování datových zpráv.

Platné hodnoty:

- MD5
- SHA-1
- SHA-2 Rodina:
  - SHA256
  - SHA384 (minimální délka klíče je přijatelná-768 bitů)
  - SHA512 (minimální délka klíče je přijatelná-768 bitů)

Zásada, která neuvádí podpisový algoritmus, nebo určuje algoritmus NONE, znamená, že zprávy umístěné ve frontě přidružené k zásadě nejsou podepsány.

Poznámka: Kvalita ochrany použitá pro funkce vložení a získání zprávy se musí shodovat. Je-li mezi frontou a zprávou ve frontě zjištěna neshoda zásady kvality ochrany, zpráva se neakceptuje a je odeslána do fronty ošetření chyb. Toto pravidlo platí pro lokální i vzdálené fronty.

Algoritmus šifrování v produktu AMS

Šifrovací algoritmus označuje algoritmus, který se má použít při šifrování datových zpráv umístěných ve frontě přidružené k zásadě.

Platné hodnoty:

- RC2
- DES
- 3DES
- AES128
- AES256

Zásada, která neuvádí šifrovací algoritmus nebo určuje algoritmus NONE znamená, že zprávy umístěné ve frontě přidružené k zásadě nejsou šifrovány.

Všimněte si, že zásada, která uvádí šifrovací algoritmus jiný než NONE , musí také uvádět alespoň jedno DN příjemce a podpisový algoritmus, protože Advanced Message Security šifrované zprávy jsou také podepsány.

Důležité: Kvalita ochrany použitá pro funkce vložení a získání zprávy se musí shodovat. Je-li mezi frontou a zprávou ve frontě zjištěna neshoda zásady kvality ochrany, zpráva se neakceptuje a je odeslána do fronty ošetření chyb. Toto pravidlo platí pro lokální i vzdálené fronty.

Tolerance v produktu AMS

Atribut tolerování označuje, zda může produkt Advanced Message Security přijímat zprávy bez uvedené zásady zabezpečení.

Při načítání zprávy z fronty se zásadou pro šifrování zpráv, pokud zpráva není šifrována, je vrácena do volající aplikace. Platné hodnoty:

0
Ne (**výchozí**).

1
Ano.

Zásada, která neurčuje hodnotu tolerance nebo má hodnotu 0, znamená, že zprávy umístěné ve frontě přidružené k zásadě musí odpovídat pravidlům zásady.

Tolerance je volitelná a existuje pro usnadnění konfigurace, kdy byly zásady použity ve frontách, 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.
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 653

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.
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 651

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 zásady zabezpečení v produktu AMS

Můžete použít produkt Advanced Message Security k výběru určitého algoritmu nebo metody k ochraně dat.

Zásada zabezpečení je konceptuálním objektem, který popisuje způsob, jakým je zpráva šifrovaně šifrována a podepsána.

Tabulka 107. Atributy zásady zabezpečení v produktu 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 certifikátů (DN) potenciálních příjemců zprávy.
Kontrolní seznam DN podpisu	Seznam DN podpisů, které mají být ověřovány během načítání zpráv.

V produktu Advanced Message Securityjsou zprávy šifrovány pomocí symetrického klíče a symetrický klíč je šifrován s použitím veřejných klíčů příjemců. Veřejné klíče jsou šifrovány algoritmem RSA s klíči o efektivní délce až do 2048 bitů. Skutečné asymetrické šifrování klíče závisí na délce klíče certifikátu.

Podporované algoritmy symetrického klíče jsou následující:

- RC2
- DES
- 3DES
- AES128
- AES256

Produkt Advanced Message Security také podporuje následující kryptografické transformační funkce:

- MD5
- SHA-1
- SHA-2 Rodina:
  - SHA256
  - SHA384 (minimální délka klíče je přijatelná-768 bitů)
  - SHA512 (minimální délka klíče je přijatelná-768 bitů)

Poznámka: Kvalita ochrany použitá pro funkce vložení a získání zprávy se musí shodovat. Je-li mezi frontou a zprávou ve frontě zjištěna neshoda zásady kvality ochrany, zpráva se neakceptuje a je odeslána do fronty ošetření chyb. Toto pravidlo platí pro lokální i vzdálené fronty.

Kvalita ochrany v produktu AMS

Advanced Message Security zásady ochrany dat znamenají kvalitu ochrany (QOP).

Tři úrovně ochrany v produktu Advanced Message Security jsou doplněny o čtvrtou úroveň v produktu IBM MQ 9.0 a později a všechny závislé na šifrovacích algoritmech, které se používají k podepisování a šifrování zprávy:

- Soukromí-zprávy umístěné ve frontě musí být podepsány a šifrovány.
- Integrita-zprávy umístěné ve frontě musí být podepsány odesílatelem.
- Utajení-zprávy umístěné ve frontě musí být šifrovány. Další informace naleznete v tématu “Kvality ochrany dostupné s AMS” na stránce 581
- Žádná-žádná ochrana dat není použitelná.

Zásada, která stanovuje, že zprávy musí být podepsány, když jsou umístěna ve frontě, má QOP INTEGRITY. QOP INTEGRITY znamená, že zásada určuje podpisový algoritmus, ale neurčuje šifrovací algoritmus. Na zprávy chráněné integrity se také odkazuje jako na "SIGNED".

Zásada, která stanovuje, že zprávy musí být podepsány a šifrovány, když jsou umístěny na frontě, má QOP z PRIVACY. QOP z PRIVACY znamená, že když zásada stanovuje podpisový algoritmus a šifrovací algoritmus. Na zprávy chráněné ochranou osobních údajů se odkazuje také jako na "SEALED".

Zásada, která určuje, že zprávy musí být při umístění do fronty šifrovány, má hodnotu QOP CONFIDENTIALITY. QOP CONFIDENTIALITY znamená, že zásada určuje šifrovací algoritmus.

Zásada, která nestanovuje podpisový algoritmus nebo šifrovací algoritmus, má QOP typu NONE. Produkt Advanced Message Security neposkytuje žádnou ochranu dat pro fronty, které mají zásadu s QOP typu NONE.

Správa zásad zabezpečení v produktu AMS

Zásada zabezpečení je konceptuálním objektem, který popisuje způsob, jakým je zpráva šifrovaně šifrována a podepsána.

Umístění, ze kterého jsou spuštěny všechny administrativní úlohy související se zásadami zabezpečení, závisí na platformě, kterou používáte.

- ALW V systému AIX, Linux, and Windowsmůžete ke správě zásad zabezpečení použít příkazy DELETE POLICY, DISPLAY POLICYa SET POLICY (nebo ekvivalentní příkazy PCF).
  - Linux AIX V systému AIX and Linuxlze administrativní úlohy spouštět z produktu *MQ_INSTALLATION_PATH*/bin.
  - Windows Na platformách Windows lze administrativní úlohy spouštět z libovolného umístění, protože proměnná prostředí PATH se aktualizuje při instalaci.
- IBM i V systému IBM ijsou příkazy DSPMQMSPL, SETMQMSPLa WRKMQMSPL instalovány do systémové knihovny QSYS pro primární jazyk systému, je-li nainstalován produkt IBM MQ .

  Další národní jazykové verze se instalují do knihoven QSYS29xx v závislosti na zavádění jazykových funkcí. Například počítač s americkou angličtinou jako primární jazyk a korejština jako sekundární jazyk má nainstalované americké anglické příkazy do knihovny QSYS a korejský sekundární jazyk zavedení v QSYS2962 jako 2962 je jazykovým zatížením korejštiny.
- z/OS V systému z/OSjsou administrativní příkazy spuštěny pomocí obslužného programu zásad zabezpečení zpráv (CSQ0UTIL). Když jsou zásady vytvořeny, upraveny nebo odstraněny na z/OS, změny nejsou rozpoznány produktem Advanced Message Security , dokud není správce front zastaven a restartován, nebo se příkaz z/OS MODIFY použije k aktualizaci konfigurace zásad Advanced Message Security . Příklad:

```
F <qmgr ssid>AMSM,REFRESH POLICY
```

Související úlohy

“Vytvoření zásad zabezpečení v produktu AMS” na stránce 656
Zásady zabezpečení definují způsob, jakým je zpráva chráněna při vložení zprávy, nebo způsob, jakým musí být zpráva chráněna při přijetí zprávy.

“Změny zásad zabezpečení v produktu AMS” na stránce 656
Pomocí produktu Advanced Message Security můžete změnit podrobnosti o zásadách zabezpečení, které jste již definovali.

“Zobrazení a výpis zásad zabezpečení v produktu AMS” na stránce 657
Příkaz **dspmqspl** se používá k zobrazení seznamu všech zásad zabezpečení nebo podrobných informací o pojmenované zásadě v závislosti na parametrech příkazového řádku, které zadáte.

“Odebrání zásad zabezpečení v produktu AMS” na stránce 659
Chcete-li odebrat zásady zabezpečení v produktu Advanced Message Security, je třeba použít příkaz `setmqspl` .

Provoz Advanced Message Security

Související odkazy

Obslužný program zásad zabezpečení zpráv (CSQ0UTIL)

Vytvoření zásad zabezpečení v produktu AMS

Zásady zabezpečení definují způsob, jakým je zpráva chráněna při vložení zprávy, nebo způsob, jakým musí být zpráva chráněna při přijetí zprávy.

Než začnete

Při vytváření zásad zabezpečení je třeba splnit některé vstupní podmínky:

- Správce front musí být spuštěn.
- Název zásady zabezpečení musí dodržovat Pravidla pojmenování objektů IBM MQ.
- Musíte mít potřebné oprávnění pro připojení ke správci front a vytvoření zásady zabezpečení:
  - z/OS V systému z/OSudělte oprávnění dokumentované v tématu Obslužný program zásad zabezpečení zpráv (CSQ0UTIL).
  - Multi Na jiných platformách jiných než z/OSje třeba pomocí příkazu setmqaut udělit potřebné oprávnění + connect, + inq a + chg.

  Další informace o konfiguraci zabezpečení viz “Nastavení zabezpečení” na stránce 125.
- z/OS V systému z/OSzajistěte, aby vyžadované systémové objekty byly definovány v souladu s definicemi v souboru CSQ4INSM.

Příklad

Zde je uveden příklad vytvoření zásady pro správce front QMGR. Zásada určuje, že zprávy mají být podepsány pomocí algoritmu SHA256 a šifrovány 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 produktu 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 uveden příklad vytváření zásad ve správci front QMGR. Zásada určuje, že zprávy budou šifrovány pomocí algoritmu 3DES pro certifikáty s DN: CN=john, O=IBM, C=US a CN=jeff, O=IBM, C=US a podepsána s 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 použitá pro vložení zprávy a získání si musí odpovídat. Je-li kvalita zásady ochrany, která je definovaná pro zprávu, slabší než ta definovaná pro frontu, zpráva se odešle do fronty ošetření chyb. Tato zásada platí jak pro lokální, tak pro vzdálené fronty.

Související odkazy

Úplný seznam atributů příkazu setmqspl

Změny zásad zabezpečení v produktu AMS

Pomocí produktu Advanced Message Security můžete změnit podrobnosti o zásadách zabezpečení, které jste již definovali.

Než začnete

- Správce front, v němž chcete pracovat, musí být spuštěn.
- Musíte mít potřebné oprávnění pro připojení ke správci front a vytvořit zásadu zabezpečení.

– z/OS V systému z/OSudělte oprávnění dokumentované v tématu Obslužný program zásad zabezpečení zpráv (CSQ0UTIL).

– Multi Na jiných platformách jiných než z/OSje třeba pomocí příkazu setmqaut udělit potřebné oprávnění + connect, + inq a + chg.

Další informace o konfiguraci zabezpečení viz “Nastavení zabezpečení” na stránce 125.

Informace o této úloze

Chcete-li změnit zásady zabezpečení, použijte příkaz `setmqspl` na již existující zásadu poskytující nové atributy.

Příklad

Zde je uveden příklad vytvoření zásady s názvem MYQUEUE ve správci front s názvem QMGR, který určuje, že zprávy mají být šifrovány pomocí algoritmu 3DES pro autory (**-a**) s certifikáty s rozlišujícím názvem (DN) CN=alice, O=IBM, C=US a podepsány algoritmem SHA256 pro příjemce (**-r**) s certifikáty s DN 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 tuto zásadu změnit, zadejte příkaz `setmqspl` se všemi atributy z příkladu, který mění pouze ty 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 zásady zabezpečení)

Zobrazení a výpis zásad zabezpečení v produktu AMS

Příkaz **dspmqspl** se používá k zobrazení seznamu všech zásad zabezpečení nebo podrobných informací o pojmenované zásadě v závislosti na parametrech příkazového řádku, které zadáte.

Než začnete

- Chcete-li zobrazit podrobnosti o zásadách zabezpečení, musí existovat správce front a musí být spuštěn.
- Musíte mít potřebné oprávnění pro připojení ke správci front a vytvořit zásadu zabezpečení.
  – z/OS V systému z/OSudělte oprávnění dokumentované v tématu Obslužný program zásad zabezpečení zpráv (CSQ0UTIL).
  – Multi Na jiných platformách jiných než z/OSje třeba pomocí příkazu setmqaut udělit potřebné oprávnění + connect, + inq a + chg.

  Další informace o konfiguraci zabezpečení viz “Nastavení zabezpečení” na stránce 125.

Informace o této úloze

Následuje seznam příznaků příkazu **dspmqspl** :

*Tabulka 108. Parametry příkazu **dspmqspl** .*

Příznak příkazu	Vysvětlení
-m	Název správce front (povinný).
-p	Název zásady.

*Tabulka 108. Parametry příkazu **dspmqspl** . (pokračování)*	
Příznak příkazu	**Vysvětlení**
-export	Přidání tohoto parametru generuje výstup, který lze snadno použít na jiného správce front.

Příklad

Následující příklad ukazuje, jak vytvořit dvě zásady zabezpečení pro produkt `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 ukazuje příkaz, který zobrazuje podrobnosti o všech zásadách definovaných pro `venus.queue.manager` a o výstupu, který produkuje:

```
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 ukazuje příkaz, který zobrazuje podrobnosti o zvolené 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 vyexportujete zásadu pomocí parametru **-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/OSje exportovaná informace o zásadě zapsána do souboru CSQ0UTIL k příkazu 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 zásady zabezpečení:

- Linux AIX V systému AIX and Linux:
  1. Přihlaste se jako uživatel, který patří do administrativní skupiny produktu `mqm` IBM MQ .
  2. Zadejte příkaz `. policies.sh`.
- Windows V systému Windowsspusťte příkaz `policies.bat`.
- z/OS V produktu z/OS použijte obslužný program CSQ0UTIL , který uvádí SYSIN datovou sadu obsahující exportované informace o zásadě.

Související odkazy
Úplný seznam atributů příkazu dspmqspl

Odebrání zásad zabezpečení v produktu AMS
Chcete-li odebrat zásady zabezpečení v produktu Advanced Message Security, je třeba použít příkaz `setmqspl` .

Než začnete
Existují některé vstupní podmínky, které musí být splněny při správě zásad zabezpečení:

- Správce front musí být spuštěn.
- Musíte mít potřebné oprávnění pro připojení ke správci front a vytvořit zásadu zabezpečení.
  - z/OS V systému z/OSudělte oprávnění dokumentované v tématu Obslužný program zásad zabezpečení zpráv (CSQ0UTIL).
  - Multi Na jiných platformách jiných než z/OSje třeba pomocí příkazu setmqaut udělit potřebné oprávnění + connect, + inq a + chg.

  Další informace o konfiguraci zabezpečení viz “Nastavení zabezpečení” na stránce 125.

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 systémových front v produktu AMS

Systémové fronty umožňují komunikaci mezi produktem IBM MQ a jeho pomocnými aplikacemi. Kdykoli je vytvořen správce front, vytvoří se také systémová fronta pro ukládání interních zpráv a dat produktu IBM MQ . Systémové fronty můžete chránit pomocí produktu Advanced Message Security tak, aby k nim mohli přistupovat pouze autorizovaní uživatelé nebo je dešifrovat.

Ochrana systémové fronty se řídí stejným vzorem jako ochrana běžných front. Viz “Vytvoření zásad zabezpečení v produktu AMS” na stránce 656.

Windows Chcete-li použít ochranu systémové fronty na serveru Windows, zkopírujte soubor `keystore.conf` do následujícího adresáře:

```
c:\Documents and Settings\Default User\.mqs\keystore.conf
```

z/OS Chcete-li v produktu z/OSposkytnout ochranu pro produkt `SYSTEM.ADMIN.COMMAND.QUEUE`, musí mít příkazový server přístup k serveru `keystore` a k serveru `keystore.conf`, který obsahuje klíče a konfiguraci, aby mohl příkazový server přistupovat k klíčům a certifikátům. Všechny změny provedené v zásadě zabezpečení produktu `SYSTEM.ADMIN.COMMAND.QUEUE` vyžadují restartování příkazového serveru.

Všechny zprávy odeslané a přijaté z fronty příkazů jsou podepsány nebo podepsány a šifrovány v závislosti na nastavení zásad. Pokud administrátor definuje oprávněné podepisující subjekty, zprávy příkazu, které nepředávají kontrolu rozlišujícího názvu (DN) podepisujícího subjektu, nejsou spuštěny příkazovým serverem a nejsou směrovány do fronty ošetření chyb produktu Advanced Message Security . Zprávy, které jsou odeslány jako odpovědi na dočasné dynamické fronty programu Průzkumník produktu IBM MQ , 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 9.2.3 Kontinuální fronty a AMS

Je možné, aby bylo možné proudovat duplicitní zprávy chráněné produktem Advanced Message Security (AMS).

Pokud má fronta definovanou zásadu AMS , která způsobí podpis a/nebo zašifrování zpráv vložených do této fronty, můžete také nakonfigurovat atribut **STREAMQ** fronty tak, aby naložil kopii každé chráněné zprávy do druhé fronty. Duplikát, kontinuální zpráva je podepsána a/nebo šifrována pomocí stejné zásady, která byla nakonfigurována pro původní frontu.

V následujícím příkladu konfigurujete dvě fronty: QUEUE1 a QUEUE2. QUEUE1 má svůj atribut **STREAMQ** nakonfigurovaný tak, aby vkládal zprávy do QUEUE2:

```
DEFINE QLOCAL(QUEUE2)

DEFINE QLOCAL(QUEUE1) STREAMQ(QUEUE2)
```

Chráněné zprávy produktu AMS jsou do QUEUE1 vloženy 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 spotřebovávat zprávy z QUEUE2.

QUEUE1 má na něj následující AMS zásady ochrany soukromí:

```
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 zahrnout jak příjemce původních zpráv z QUEUE1, tak příjemců, kteří budou spotřebovávat duplicitní zprávy z QUEUE2.

Když se aplikace pokusí spotřebovávat zprávy z QUEUE2 provádí kontroly integrity a/nebo dešifruje zprávu založenou na zásadě, která byla nastavena na QUEUE2. Pokud chce aplikace spotřebovávat proudové zprávy z QUEUE2, musíte nastavit vhodnou zásadu na QUEUE2 , která umožňuje kontrolu integrity zpráv a dešifrování správně.

Konkrétně, podpisový algoritmus, podepisující subjekt a šifrovací algoritmus musí být stejné, jako zásada použitá na QUEUE1. Příjemci zásady pro QUEUE2 musí obsahovat identitu příjemce, který tuto zprávu spotřebovává, z QUEUE2.

Poznámka: Není nutné, aby se zásada použila na QUEUE2 , aby se vypsali všechny příjemce pojmenované 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 zprávy chráněné 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

Streaming front

Udělení oprávnění OAM v produktu AMS

Oprávnění k souboru autorizují všechny uživatele k provedení příkazů `setmqspl` a `dspmqspl` . Produkt Advanced Message Security však spoléhá na správce oprávnění objektu (OAM) a každý pokus o provedení těchto příkazů uživatelem, který nepatří do skupiny mqm, která je skupinou administrace produktu IBM MQ , nebo nemá oprávnění číst nastavení zásad zabezpečení, která jsou udělena, a dojde 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: Tyto 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: Oprávnění k procházení slouží k SYSTEM.PROTECTION.POLICY.QUEUE není povinná ve všech situacích. Produkt IBM MQ optimalizuje výkon pomocí zásad ukládání do mezipaměti, takže nemusíte procházet záznamy o podrobnostech zásady v systému SYSTEM.PROTECTION.POLICY.QUEUE ve všech případech.

Produkt IBM MQ neukládá do mezipaměti všechny dostupné zásady. Existuje-li vysoký počet zásad, produkt IBM MQ ukládá omezený počet zásad do mezipaměti. Má-li tedy správce front definován nízký počet definovaných zásad, není třeba zadávat volbu procházení do systému SYSTEM.PROTECTION.POLICY.QUEUE.

Do této fronty byste však měli udělit oprávnění k procházení, v případě, že je definován vysoký počet zásad, nebo pokud používáte staré klienty. SYSTEM.PROTECTION.ERROR.QUEUE se používá k vložení chybových zpráv generovaných kódem AMS. Oprávnění k vložení pro tuto frontu se kontroluje pouze tehdy, když se pokusíte vložit chybovou zprávu do fronty. Při pokusu o vložení nebo získání zprávy z chráněné fronty AMS se nekontroluje vaše oprávnění k zařazení do fronty.

Udělení oprávnění zabezpečení v produktu AMS

Při použití zabezpečení prostředků příkazu je třeba nastavit oprávnění tak, aby umožňovala funkci produktu Advanced Message Security fungovat. Toto téma používá příkazy RACF v příkladech. Pokud váš podnik používá jiného externího správce zabezpečení (ESM), musíte použít ekvivalentní příkazy pro tento modul ESM.

Pro udělení oprávnění zabezpečení existují tři aspekty:

- “Adresní prostor AMSM” na stránce 663
- “CSQ0UTIL” na stránce 663
- “Použití front, které mají definovanou zásadu Advanced Message Security” na stránce 664

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* -Toto může být název skupiny.
3. Příklady zobrazují třídu MQQUEUE. Toto může být také MXQUEUE, GMQQUEUE nebo GMXQUEUE. Další informace viz “Profily pro zabezpečení fronty” na stránce 194.

Navíc, pokud profil již existuje, nevyžadujete příkaz RDEFINE.

Adresní prostor AMSM

Je třeba zadat zabezpečení produktu IBM MQ pro jméno uživatele, pod kterým je adresový prostor Advanced Message Security spuštěn.

- 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 SYSTEM.PROTECTION.POLICY.QUEUE, zadejte:

```
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 SYSTEM.PROTECTION.POLICY.QUEUE, vyžadovaná pro příkaz **setmqpol** , vydání:

```
  RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE UACC(NONE)
              PERMIT QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(ALTER)
```

- Pro přístup k SYSTEM.PROTECTION.POLICY.QUEUE, vyžadovaná pro příkaz **dspmqpol** , vydání:

```
  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 práci s frontami, které mají definovánu zásadu, která má definovanou zásadu, vyžaduje tato aplikace dodatečná oprávnění k tomu, aby produkt Advanced Message Security mohl chránit zprávy.

Aplikace vyžaduje:

- Přístup pro čtení v aplikaci SYSTEM.PROTECTION.POLICY.QUEUE. Postupujte takto:

```
RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE UACC(NONE)
         PERMIT QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(READ)
```

- Přístup k objektu SYSTEM.PROTECTION.ERROR.QUEUE. Postupujte takto:

```
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 produkt AMS v systému IBM i

Prvním úkolem při nastavení ochrany produktu Advanced Message Security je vytvoření certifikátu a jeho přidružení k vašemu prostředí. Přidružení je nakonfigurováno prostřednictvím souboru drženého v integrovaném systému souborů (IFS).

Postup

1. Chcete-li vytvořit certifikát podepsaný držitelem pomocí nástrojů OpenSSL dodávaného s produktem IBM i, zadejte z prostředí QShell tento příkaz:

   ```
   /QOpenSys/usr/bin/openssl req -x509 -newkey rsa:2048 -keyout
   $HOME/private.pem -out $HOME/mycert.pem -nodes -days 365
   ```

   Příkaz vás vyzve k zadání různých atributů rozlišujícího názvu pro nový certifikát podepsaný svým držitelem, včetně:

   - Běžné jméno (CN =)
   - Organizace (O =)
   - Země (C =)

   Tím se vytvoří nešifrovaný soukromý klíč a odpovídající certifikát, a to jak ve formátu PEM (Privacy Enhanced Mail).

   Pro zjednodušení 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 argumentem **-config** . Další podrobnosti o syntaxi konfiguračního souboru najdete v dokumentaci 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 jak certifikát, tak 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 produktu $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 musejí být přidruženy k vašemu prostředí vytvořením konfiguračního souboru úložiště klíčů `keystore.conf`ve vašem výchozím umístění.

   Produkt AMS standardně hledá 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 v systému IBM i*

Před vytvořením zásady je třeba vytvořit frontu, která bude obsahovat chráněné zprávy.

Postup

1. Na příkazový řádek zadejte příkaz;

```
CRTMQMQ QNAME(PROTECTED) QTYPE(*LCL) MQMNAME (mqmname)
```

   kde mqmname je název vašeho správce front.

   Použijte příkaz DSPMQM a 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, která je dosažena vytvořením zásady s algoritmem digitálního podpisu, ale bez šifrovacího algoritmu.

   Zprávy jsou podepsány, ale nejsou šifrovány. Mají-li být zprávy šifrovány, je třeba určit šifrovací algoritmus a jeden nebo více zamýšlených příjemců zprávy.

   Certifikát ve veřejném úložišti klíčů pro požadovaného příjemce zprávy je identifikován pomocí rozlišujícího názvu.

2. Zobrazte rozlišující názvy certifikátů ve veřejném úložišti klíčů, `mycert.pem` v produktu $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 požadovaného příjemce a název zásady se musí shodovat s názvem fronty, který má být chráněn.

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 vhozeny, procházeny nebo destruktivně odebrané přes tento název fronty, jsou předmětem zásady AMS .

Související odkazy

Zobrazení správce front zpráv (DSPMQM)

Nastavení zásady zabezpečení MQM (SETMQMSPL)

IBM i *Testování zásady pro AMS v systému IBM i*

Použijte ukázkové aplikace dodávané spolu s produktem k testování zásad zabezpečení.

Informace o této úloze

Můžete použít ukázkové aplikace dodávané s produktem IBM MQ , například AMQSPUT4, AMQSGET4, AMQSGBR4a nástroje jako WRKMQMMSG pro vložení, procházení a získání zpráv s použitím názvu fronty PROTECTED.

Za předpokladu, že bylo vše správně nakonfigurováno, nemělo by existovat žádný rozdíl v chování aplikace u nechráněné fronty pro tohoto uživatele.

Uživatel není nastaven pro Advanced Message Securitynebo uživatel, který nemá požadovaný soukromý klíč k dešifrování zprávy, však nebude schopen zobrazit zprávu. Uživatel obdrží kód dokončení RCFAIL, který odpovídá 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 příkazu AMQSPUT0. Pak můžete vytvořit alias frontu pro procházení nezpracovaných chráněných dat, zatímco ve zbytku.

Postup

Chcete-li uživateli udělit nezbytná oprávnění, spusťte:

```
CRTMQMQ QNAME(ALIAS) QTYPE(*ALS) TGTQNAME(PROTECTED) MQMNAME(yourqm)
```

Procházení s použitím názvu fronty ALIAS, například pomocí příkazu AMQSBCG4 nebo WRKMQMMSG, by mělo odhalit větší počet zpráv produktu scrambled , pokud procházení fronty PROTECTED zobrazuje zprávy cleartext.

Zmašované zprávy jsou viditelné, ale původní prostý text není dešifrován pomocí fronty ALIAS, protože neexistuje žádná zásada pro server AMS, která by vynutila shodu s tímto názvem. Proto jsou vrácena prvotní chráněná data.

Související odkazy

Nastavení zásady zabezpečení MQM (SETMQMSPL)

Práce se zprávami MQ (WRKMQMMSG)

Události příkazů a konfigurace pro produkt AMS

Pomocí produktu Advanced Message Securitymůžete generovat zprávy událostí příkazů a konfiguračních událostí, které mohou být protokolovány a sloužit jako záznam změn zásad pro auditování.

Události příkazu a konfigurace generované produktem IBM MQ jsou zprávy o formátu PCF odeslaného do vyhrazených front ve správci front, ve kterém došlo k dané události.

Zprávy událostí konfigurace jsou odeslány na SYSTEM.ADMIN.CONFIG.EVENT .

Zprávy událostí příkazu se odesílají do SYSTEM.ADMIN.COMMAND.EVENT .

Události se generují bez ohledu na nástroje, které používáte ke správě zásad zabezpečení produktu Advanced Message Security .

V produktu Advanced Message Securityexistují čtyři typy událostí generovaných různými akcemi na zásadách zabezpečení:

- “Vytvoření zásad zabezpečení v produktu AMS” na stránce 656, které generují dvě zprávy událostí produktu IBM MQ :
  - Událost konfigurace
  - Událost příkazu
- “Změny zásad zabezpečení v produktu AMS” na stránce 656, který generuje tři zprávy událostí produktu 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 produktu AMS” na stránce 657, který generuje jednu zprávu události IBM MQ :
  - Událost příkazu
- “Odebrání zásad zabezpečení v produktu AMS” na stránce 659, který generuje dvě zprávy událostí produktu IBM MQ :
  - Událost konfigurace
  - Událost příkazu

Povolení a zakázání protokolování událostí pro produkt AMS

Příkazy a konfigurační události můžete řídit pomocí atributů správce front **CONFIGEV** a **CMDEV**. Chcete-li tyto události povolit, nastavte příslušný atribut správce front na hodnotu ENABLED. Chcete-li tyto události zakázat, nastavte příslušný atribut správce front na hodnotu DISABLED.

Postup

Události konfigurace

Chcete-li povolit události konfigurace, nastavte **CONFIGEV** na ENABLED. Chcete-li zakázat události konfigurace, nastavte **CONFIGEV** na DISABLED. Konfigurační události můžete povolit například pomocí následujícího příkazu MQSC:

```
ALTER QMGR CONFIGEV (ENABLED)
```

Události příkazů

Chcete-li povolit události příkazů, nastavte **CMDEV** na ENABLED. Chcete-li povolit příkazovým událostem pro příkazy kromě příkazů **DISPLAY MQSC** a Dotaz na příkazy PCF, nastavte parametr

CMDEV na hodnotu NOBRAZIT. Chcete-li zakázat události příkazů, nastavte parametr **CMDEV** na hodnotu DISABLED. Můžete například povolit události příkazů pomocí následujícího příkazu MQSC:

```
ALTER QMGR CMDEV (ENABLED)
```

Související úlohy

Řízení událostí konfigurace, příkazů a modulu protokolování v produktu IBM MQ

Formát zprávy události příkazu pro AMS

Zpráva o události příkazu se skládá ze struktury MQCFH a z parametrů PCF za ním.

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 jsou vždy dva parametry typu MQCFGR (skupina). Každá skupina se skládá z odpovídajících 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. (Toto je 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 z příkazové zprávy).
Identifikátor:	MQCACF_EVENT_USER_ID.
Datový typ:	MQCFST.
Maximální délka:	MQ_USER_ID_LENGTH.
Vráceno:	Jako vždycky.

EventOrigin

Popis:	Původ akce způsobující událost.
Identifikátor:	MQIACF_EVENT_ORIGIN.
Datový typ:	MQCFIN.
Hodnoty:	**MQEVO_CONSOLE** Příkazový řádek konzoly. **MQEVO_MSG** Příkazová zpráva z modulu plug-in IBM MQ Explorer .
Vráceno:	Jako vždycky.

EventQMgr

Popis:	Správce front, ve kterém byl zadán příkaz nebo volání. (Správce front, ve kterém je příkaz spuštěn 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: Jako vždycky.

EventAccountingToken

Popis: Pro příkazy přijaté jako zprávu (MQEVO_MSG), účtovací token (AccountingToken) z MD z příkazové zprávy.

Identifikátor: MQBAKF_EVENT_ACCOUNTING_TOKEN.

Datový typ: MQCFBS.

Maximální délka: MQ_ACCOUNTING_TOKEN_LENGTH.

Vráceno: Pouze pokud EventOrigin je MQEVO_MSG.

Data EventIdentity

Popis: Pro příkazy přijaté jako zpráva (MQEVO_MSG), data identity aplikace (ApplIdentityData), z MD zprávy příkazu.

Identifikátor: IDENTITA MQCACF_EVENT_APPL_IDENTITY.

Datový typ: MQCFST.

Maximální délka: HODNOTA MQ_APPL_IDENTITY_DATA_LENGTH.

Vráceno: Pouze pokud EventOrigin je MQEVO_MSG.

EventApplType

Popis: Pro příkazy přijaté jako zprávu (MQEVO_MSG), typ aplikace (PutApplType) z MD z příkazové zprávy.

Identifikátor: MQIACF_EVENT_APPL_TYPE.

Datový typ: MQCFIN.

Vráceno: Pouze pokud EventOrigin je MQEVO_MSG.

EventApplName

Popis: Pro příkazy přijaté jako zprávu (MQEVO_MSG) je název aplikace (PutApplName) z MD z příkazové zprávy.

Identifikátor: MQCACF_EVENT_APPL_NAME.

Datový typ: MQCFST.

Maximální délka: MQ_APPL_NAME_LENGTH.

Vráceno: Pouze pokud EventOrigin je MQEVO_MSG.

EventApplOrigin

Popis: Pro příkazy přijaté jako zprávu (MQEVO_MSG), data původu aplikace (ApplOriginData) z MD z příkazové zprávy.

Identifikátor: MQCACF_EVENT_APPL_ORIGIN.

Datový typ: MQCFST.

Maximální délka: MQ_APPL_ORIGIN_DATA_LENGTH.

Vráceno: Pouze pokud EventOrigin je MQEVO_MSG.

Příkaz

Popis: Kód příkazu.

Identifikátor: MQIACF_COMMAND.

Datový typ: MQCFIN.

Hodnoty: **číselná hodnota MQCMD_INQUIRE_PROT_POLICY 205**
Numerická hodnota MQCMD_CREATE_PROT_POLICY 206
Numerická hodnota MQCMD_DELETE_PROT_POLICY 207
numerická hodnota MQCMD_CHANGE_PROT_POLICY 208
Ty jsou definovány v produktu IBM MQ 8.0 `cmqcfc.h`

Vráceno: Jako vždycky.

Příkaz CommandData obsahuje prvky PCF, které obsahují příkaz PCF.

Formát zprávy události konfigurace pro AMS

Události konfigurace jsou zprávami PCF standardního formátu Advanced Message Security .

Možné hodnoty deskriptoru zpráv MQMD lze nalézt v Message Message MQMD (message descriptor).

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 z struktury MQCFH a struktury parametrů, která za ní následuje. Možné hodnoty MQCFH lze nalézt ve zprávě 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. (Toto je 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 z příkazové zprávy).

Identifikátor: **MQCACF_EVENT_USER_ID**

Datový typ: MQCFST.

Maximální délka: MQ_USER_ID_LENGTH.

Vráceno: Jako vždycky.

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: Jako vždycky.

EventOrigin

Popis: Původ akce způsobující událost.

Identifikátor: **MQIACF_EVENT_IGIN**

Datový typ: MQCFIN.

Hodnoty:

MQEVO_CONSOLE
Příkazový řádek konzoly.

MQEVO_MSG
Příkazová zpráva z modulu plug-in průzkumníka produktu IBM MQ .

Vráceno: Jako vždycky.

EventQMgr

Popis: Správce front, ve kterém byl zadán příkaz nebo volání. (Správce front, ve kterém je příkaz spuštěn a který generuje událost, je v MD zprávy události).

Identifikátor: **MQCACF_EVENT_Q_MGR**

Datový typ: MQCFST

Maximální délka: DÉLKA_MGR_NÁZVU_MQ_QM

Vráceno: Jako vždycky.

ObjectType

Popis: Typ objektu.

Identifikátor: **MQIACF_OBJECT_TYPE**

Datový typ: MQCFIN

Hodnota:

MQOT_PROTO_POLICY
Zásada ochrany Advanced Message Security . **1019** -Číselná hodnota definovaná v souboru IBM MQ 8.0 nebo v souboru `cmqc.h` .

Vráceno: Jako vždycky.

PolicyName

Popis: Název zásady produktu Advanced Message Security .

Identifikátor: **MQCA_POLICY_NAME**.

Datový typ: MQCFST.

Hodnota: **2112** -Číselná hodnota definovaná v souboru IBM MQ 8.0 nebo v souboru `cmqc.h` .

Maximální délka: MQ_OBJECT_NAME_LENGTH.

Vráceno: Jako vždycky.

PolicyVersion

Popis:	Verze zásady produktu Advanced Message Security .
Identifikátor:	**MQIA_POLICY_VERSION**
Datový typ:	MQCFIN
Hodnota	**238** -číselná hodnota definovaná v IBM MQ 8.0 nebo v souboru `cmqc.h` .
Vráceno:	Vždy

TolerateFlag

Popis:	Příznak tolerance zásad Advanced Message Security .
Identifikátor:	**Objekt MQIA_TOLEERATE_UNPROTECTED**
Datový typ:	MQCFIN
Hodnota	**235** -číselná hodnota definovaná v IBM MQ 8.0 nebo v souboru `cmqc.h` .
Vráceno:	Jako vždycky.

SignatureAlgorithm

Popis:	Algoritmus podpisu zásad produktu Advanced Message Security .
Identifikátor:	**ALGORITMUS MQIA_SIGNATURE_ALGORITHM**
Datový typ:	MQCFIN
Hodnota:	**236** -Číselná hodnota definovaná v souboru IBM MQ 8.0 nebo v souboru `cmqc.h` .
Vráceno:	Kdykoli je definován podpisový algoritmus definovaný v zásadě Advanced Message Security

EncryptionAlgorithm

Popis:	Algoritmus šifrování zásad produktu Advanced Message Security .
Identifikátor:	**MQIA_ENCRYPTION_ALGORITHM**
Datový typ:	MQCFIN
Hodnota:	**237** -Číselná hodnota definovaná v souboru IBM MQ 8.0 nebo v souboru `cmqc.h` .
Vráceno:	Kdykoli je definován šifrovací algoritmus definovaný v zásadě IBM MQ

SignerDNs

Popis:	Předmět DistinguishedName povolených podepisujících subjektů.
Identifikátor:	**ROZLIŠUJÍCÍ NÁZEV MQCA_SIGNERDN**
Datový typ:	MQCFSL
Hodnota:	**2113** -Číselná hodnota definovaná v souboru IBM MQ 8.0 nebo v souboru `cmqc.h` .
Maximální délka:	Nejdelší rozlišující název podepisujícího subjektu v zásadě, ale ne déle než MQ_DISTINGUISHED_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 souboru IBM MQ 8.0 nebo v souboru `cmqc.h` .
Maximální délka:	Nejdelší rozlišující název příjemce v zásadě, ale již není MQ_DISTINGUISHED_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 Velké Británie nebo kterékoliv jiné země, kde taková opatření odporují místním zákonům: SPOLEČNOST INTERNATIONAL BUSINESS MACHINES CORPORATION TUTO PUBLIKACI POSKYTUJE TAKOVOU, "JAKÁ 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 VYPLÝVAJÍCÍCH Z OKOLNOSTÍ. 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 spolupráce softwaru, oddělení 49XA
148 00 Praha 4-Chodby

148 00 Praha 4-Chodov
U.S.A.

Poskytnutí takových informací může být podmíněno dodržením určitých podmínek a požadavků zahrnujících v některých případech uhrazení stanoveného poplatku.

IBM poskytuje licencovaný program popsaný v těchto informacích a veškeré dostupné licencované materiály na základě podmínek smlouvy IBM Customer Agreement, IBM International Program License Agreement 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 programátorských rozhraní, jsou-li poskytovány, jsou určeny k tomu, aby vám pomohly vytvořit aplikační software pro použití s tímto programem.

Tato příručka obsahuje informace o zamýšlených programovacích rozhraních, které umožňují zákazníkům 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: Nepoužívejte tyto informace o diagnostice, úpravách a ladění jako programátorské rozhraní, protože se mohou měnit.

Ochranné známky

IBM, logo IBM , ibm.comjsou ochranné známky společnosti IBM Corporation, registrované v mnoha jurisdikcích po celém světě. Aktuální seznam ochranných známek IBM je k dispozici na webu na stránce "Copyright and trademark information"www.ibm.com/legal/copytrade.shtml. Ostatní 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 obsahuje software vyvinutý v rámci projektu Eclipse Project (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: