7.5

Zabezpečení produktu IBM WebSphere MQ

Poznámka

Než začnete používat tyto informace a produkt, který podporují, přečtěte si informace, které uvádí “Poznámky” na stránce 319.

Toto vydání se vztahuje k verzi 7, vydání 5 produktu IBM® WebSphere 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

Zabezpečení

Zabezpečení je důležitým aspektem pro vývojáře aplikací produktu IBM WebSphere MQ i pro administrátory systému, kteří konfigurují oprávnění IBM WebSphere MQ .

přehled zabezpečení

Tato kolekce témat představuje koncepce zabezpečení produktu IBM WebSphere 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 WebSphere MQ.

Bezpečnostní koncepce a mechanismy

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

Běžně přijímaná bezpečnostní opatření jsou následující:

- “Identifikace a ověřování” na stránce 5
- “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 WebSphere 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 45.

Související pojmy

“Připojení dvou správců front s použitím zabezpečení SSL nebo TLS” na stránce 201
Zabezpečené komunikace, které používají šifrovací bezpečnostní protokoly SSL nebo TLS, zahrnují nastavení komunikačních kanálů a správu digitálních certifikátů, které budete používat pro ověření.

“Práce s SSL nebo TLS” na stránce 108
Tato témata obsahují pokyny pro provádění jednotlivých úloh souvisejících s používáním SSL nebo TLS s produktem IBM WebSphere MQ.

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 WebSphere MQ , protože IBM WebSphere 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.

Produkt IBM WebSphere MQ s produktem IBM WebSphere MQ Advanced Message Security neposkytuje službu bez odmítání jako součást své základní funkce. Tato dokumentace k produktu však obsahuje návrhy na to, jak můžete v prostředí produktu WebSphere MQ zadat vlastní neodmítnou službu, a to tak, že napíšete své vlastní uživatelské programy.

Související pojmy

“Identifikace a ověření v produktu IBM WebSphere MQ” na stránce 20

V produktu IBM WebSphere 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 WebSphere MQ” na stránce 21

Oprávnění můžete použít k omezení konkrétních jednotlivců nebo aplikací ve vašem prostředí IBM WebSphere 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 48 a přidružených dílčích tématech.

Související pojmy

“Auditování v IBM WebSphere MQ” na stránce 21

IBM WebSphere 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 WebSphere MQ.

Výraz *entita* se používá k odkazování na správce front, klienta WebSphere MQ MQI, individuálního uživatele nebo jiného systému schopného vyměňovat si zprávy.

Související pojmy

“Šifrování v produktu IBM WebSphere MQ” na stránce 22
IBM WebSphere MQ poskytuje šifrování pomocí protokolů SSL (Secure sockets Layer) a 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*).

Viz Slovníček pojmů pro definici šifrování.

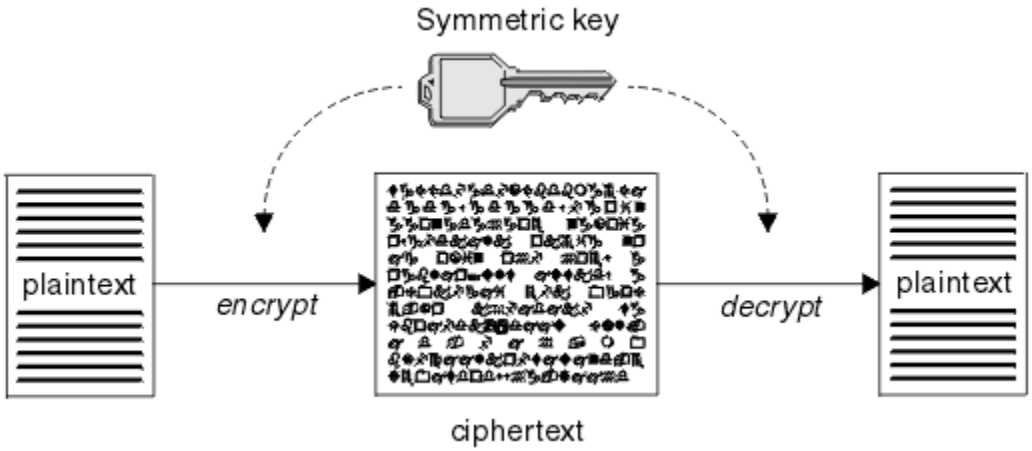
Převod zahrnuje posloupnost matematických operací, které mění vzhled zprávy během přenosu, ale nemají vliv na obsah. Kryptografické techniky mohou zajistit důvěrnost a ochranu zpráv proti neoprávněnému prohlížení (odposlouchávání), protože šifrovaná zpráva není srozumitelná. Digitální podpisy, které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

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

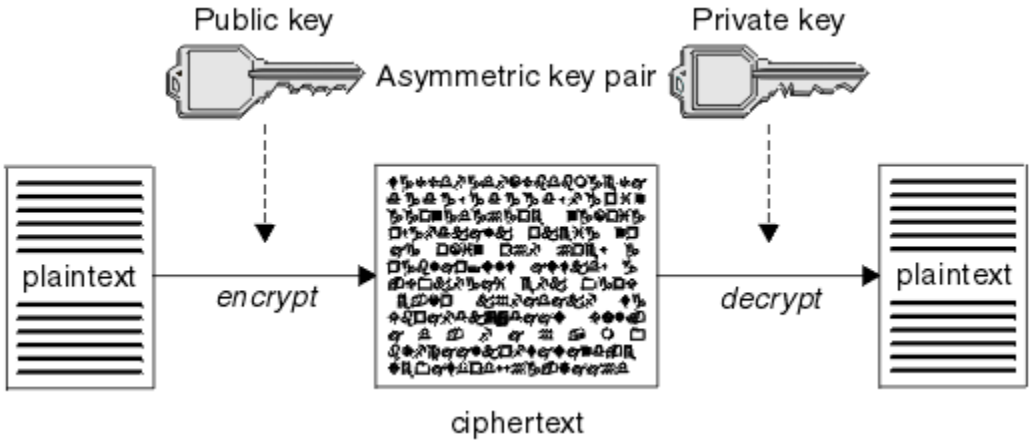
- Ty, které požadují, aby obě strany používaly stejný tajný klíč. Algoritmy, které používají sdílený klíč, jsou známé jako *symetrické* algoritmy. Obrázek 1 na stránce 8 ilustruje symetrické šifrování klíče.

- 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 klíčů, které je také známé jako *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 vypočtenou hašovací funkcí. Kód digest zprávy může být šifrován, tvoří digitální podpis.

Zprávy jsou ve své podstatě variabilní ve velikosti. Kód digest zprávy je číselným znázorněním pevné velikosti obsahu zprávy. Kód digest zprávy je vypočítán transformační funkcí, což je transformace, která splňuje dvě kritéria:

- Hašovací funkce musí být jednosměrná. 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 a 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 WebSphere MQ jsou v souladu se standardem 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, systém ji může 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 WebSphere MQ podporuje digitální certifikáty, které splňují požadavky standardu X.509 . Vyžaduje volbu ověření klienta.

Protože IBM WebSphere MQ je rovnocenný partner systému, je v terminologii SSL zobrazen jako autentizace klienta. Proto musí každý osobní certifikát používaný pro ověření SSL povolit klíčové využití 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 WebSphere MQviz “Zásady ověření platnosti certifikátu v produktu IBM WebSphere MQ” na stránce 33.

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 viz “Práce se zrušenými certifikáty” na stránce 146
- 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 .

V DN se běžně vyskytují následující typy atributů:

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 WebSphere MQ toleruje určité poškozené DN. Další informace naleznete v tématu Pravidla produktuWebSphere MQ pro hodnoty SSLPEER.

Související pojmy
“Co je v digitálním certifikátu” na stránce 10

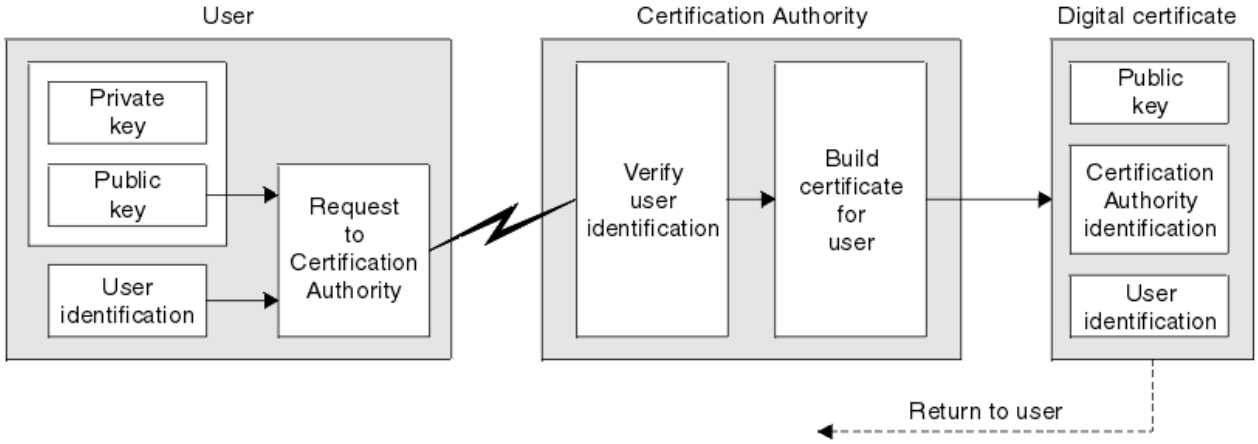
Digitální certifikáty obsahují specifické části informací určené standardem X.509 .

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 nástroj iKeyman na systémech UNIX, Linux®, a Windows a RACF na 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:

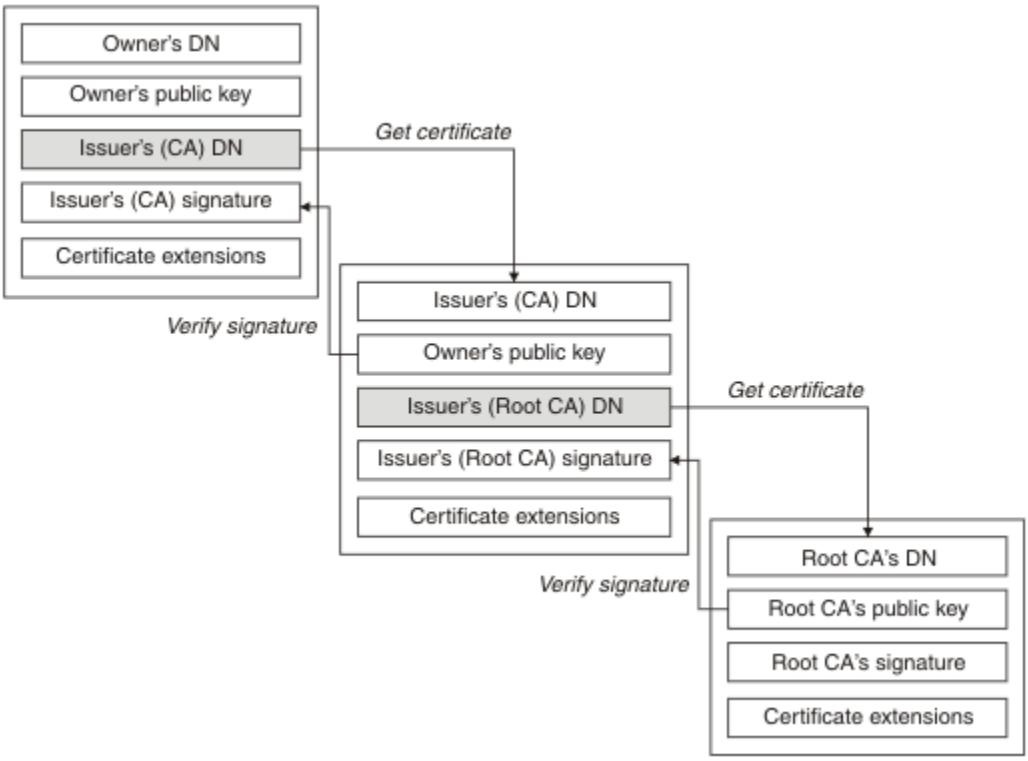
- "Identifikace uživatele" zahrnuje váš rozlišující název předmětu.
- "Identifikace certifikační autority" zahrnuje rozlišující název certifikační autority, která vydala certifikát.
-

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.

Definice vypršení platnosti certifikátu viz Slovníček pojmů .

Certifikáty mohou být odvolány z různých důvodů včetně:

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

WebSphere MQ can check whether a certificate is revoked by sending a request to an Online Certificate Status Protocol (OCSP) responder (on UNIX, Linux and Windows systems only). Případně mohou přistupovat k seznamu CRL na serveru LDAP. Informace o odvolání OCSP a CRL jsou publikovány vydavatelem certifikátů. Další informace naleznete v části “Práce se zrušenými certifikáty” na stránce 146.

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 . Ras ověřte, že 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 protokoly zabezpečení: SSL a 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). Produkt IBM WebSphere MQ podporuje zabezpečení SSL i 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 v produktu IBM WebSphere MQ” na stránce 22
IBM WebSphere MQ podporuje protokol TLS (Transport Layer Security) i protokol SSL (Secure Sockets Layer) k zajištění zabezpečení na úrovni linky pro kanály zpráv a kanály MQI.

Koncepce zabezpečení SSL (Secure Sockets Layer) a TLS (Transport Layer Security)

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

Protokoly SSL a TLS poskytují komunikační zabezpečení přes internet a umožňují 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 SSL nebo TLS je inicializováno aplikací, která se stane klientem SSL nebo TLS. Aplikace, která přijímá připojení, se stane serverem SSL nebo TLS. Každá nová relace začíná výměnou potvrzení (handshake), jak je definováno protokoly SSL nebo TLS.

Úplný seznam CipherSpecs podporovaných produktem IBM WebSphere MQ je k dispozici na adrese “Určení CipherSpecs” na stránce 213.

Další informace o protokolu SSL naleznete v informacích poskytnutých v https://www.mozilla.org/projects/security/pki/nss/ssl/draft302.txt. Další informace o protokolu TLS naleznete v informacích poskytnutých pracovní skupinou TLS na webovém serveru jednotky Internet Engineering Task Force na adrese https://www.ietf.org .

Přehled navázání komunikace SSL nebo TLS

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

Tato sekce obsahuje souhrn kroků, které umožňují vzájemnou komunikaci klienta a serveru TLS nebo SSL.

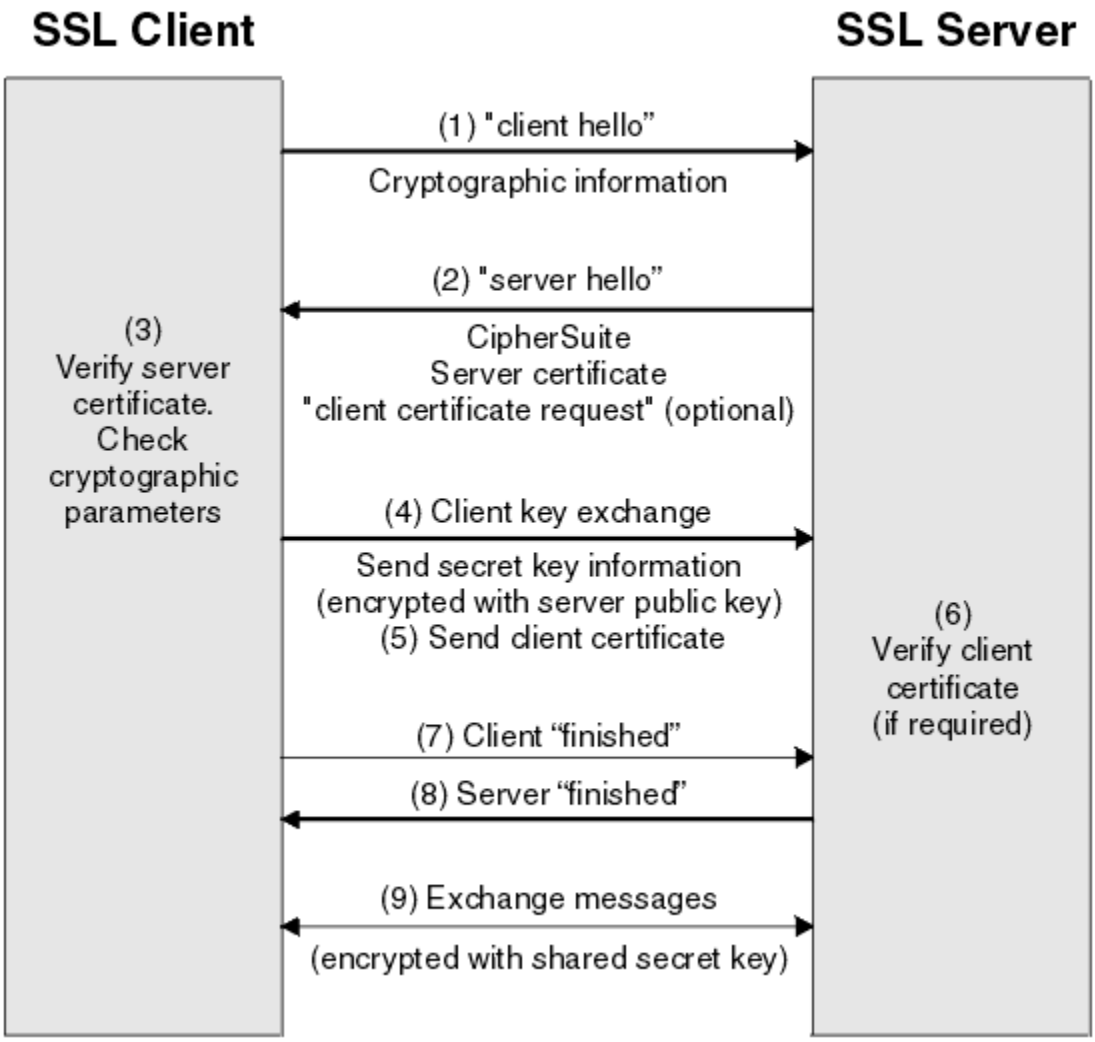
- Shodněte se na verzi protokolu, který se má použít.
- Vyberte šifrovací algoritmy.
- Proveďte vzájemnou autentizaci tím, že si vyměníte a ověřujete digitální certifikáty.
- Použijte asymetrické šifrovací techniky ke generování sdíleného tajného klíče, který se vyvaruje problému s distribucí klíčů. SSL nebo 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 přes zabezpečení SSL následující:

1. Klient SSL nebo TLS odešle zprávu "hello klienta" , která uvádí šifrovací informace, jako jsou SSL nebo TLS, a v pořadí klienta předvolby 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 SSL nebo 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 SSL nebo TLS ověřuje digitální certifikát serveru. Další informace naleznete v části “Jak SSL a TLS poskytují identifikaci, autentizaci, důvěrnost a integritu” na stránce 16.
4. Klient SSL nebo TLS odešle náhodný bajtový řetězec, který umožňuje klientovi i serveru vypočítat tajný klíč, který má být použit k šifrování následných dat zprávy. Samotný náhodný bajtový řetězec je zašifrován pomocí veřejného klíče serveru.
5. Pokud server SSL nebo TLS odeslaly "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 SSL nebo TLS ověřuje certifikát klienta. Další informace naleznete v části “Jak SSL a TLS poskytují identifikaci, autentizaci, důvěrnost a integritu” na stránce 16.
7. Klient SSL nebo TLS odešle serveru zprávu "finished" , která je zašifrována pomocí tajného klíče, což označuje, že část klienta navázání komunikace je dokončena.
8. Server SSL nebo TLS odešle klientovi zprávu "finished" , která je zašifrována pomocí tajného klíče, což indikuje, že část serveru handshake je dokončena.
9. Po dobu trvání relace SSL nebo TLS může server a klient nyní vyměňovat zprávy, které jsou symetricky šifrovány pomocí sdíleného tajného klíče.

Obrázek 5 na stránce 16 ilustruje komunikaci výměnou potvrzení SSL nebo TLS.



Obrázek 5. Přehled navázání komunikace SSL nebo TLS

Jak SSL a TLS poskytují 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 nebo TLS" na stránce 14.

Jak zabezpečení SSL a TLS poskytují 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.

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 komunikace výměnou potvrzení TLS nebo 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 SSL nebo TLS klientovi a CA Y vydává certifikát na server SSL nebo TLS:

Pouze pro ověření serveru vyžaduje server zabezpečení SSL nebo TLS:

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

a požadavky klienta SSL nebo TLS:

- Certifikát CA pro CA Y

Pokud server SSL nebo 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

Server SSL nebo TLS a 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 SSL nebo TLS ověřuje certifikát serveru a server SSL nebo TLS ověřuje certifikát klienta. K tomuto ověření jsou čtyři aspekty:

1. Digitální podpis je zkontrolován (viz “Digitální podpisy v SSL a 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 146).

Reset tajného klíče

Během komunikace výměnou potvrzení SSL nebo TLS je vygenerován *tajný klíč* pro šifrování dat mezi klientem SSL nebo TLS a serverem. 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 zabezpečení SSL a TLS poskytují důvěrnost

SSL a TLS používají kombinaci symetrického a asymetrického šifrování k zajištění utajení zpráv. Během komunikace výměnou potvrzení SSL nebo TLS se klient SSL nebo TLS a server dohodnou na použití šifrovacího algoritmu a sdíleného tajného klíče, který má být použit pouze pro jednu relaci. Všechny zprávy přenášené mezi klientem SSL nebo TLS a serverem jsou šifrovány pomocí tohoto algoritmu a klíče, což zajišťuje, že zpráva zůstane soukromá i v případě, že je zachycena. SSL podporuje širokou škálu šifrovacích algoritmů. Vzhledem k tomu, že zabezpečení SSL a TLS používají při přenášení sdíleného tajného klíče asymetrické šifrování, neexistuje žádný problém s distribucí klíčů. Další informace o technikách šifrování naleznete v tématu “Šifrování” na stránce 7.

Jak zabezpečení SSL a TLS poskytují integritu

SSL a TLS poskytují integritu dat při výpočtu kódu digest zprávy. Další informace jsou uvedeny v tématu “Integrita dat zpráv” na stránce 222.

Použití SSL nebo TLS zajišťuje integritu dat za předpokladu, že CipherSpec ve vaší definici kanálu používá hašovací algoritmus, jak je popsáno v tabulce v “Určení CipherSpecs” na stránce 213.

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 TLS nebo SSL se musí dohodnout na stejné sadě CipherSpec , aby bylo možné komunikovat.

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

Další informace o CipherSpecsviz “Určení CipherSpecs” na stránce 213.

Sada CipherSuite je sada šifrovacích algoritmů používaných připojením SSL nebo 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 nebo SSL. Název platné CipherSuite definuje kombinaci použitých algoritmů. Příklad: CipherSuite SSL_RSA_WITH_RC4_128_MD5 určuje:

- Směnný a ověřovací algoritmus RSA
- Šifrovací algoritmus RC4 používající 128bitový klíč
- Algoritmus MAC MD5

Pro výměnu klíčů a ověření je k dispozici několik algoritmů, ale algoritmus RSA je v současné době nejpoužívanější. V použitých šifrovacích algoritmech a algoritmu MAC se používá více různých algoritmů.

Digitální podpisy v SSL a TLS

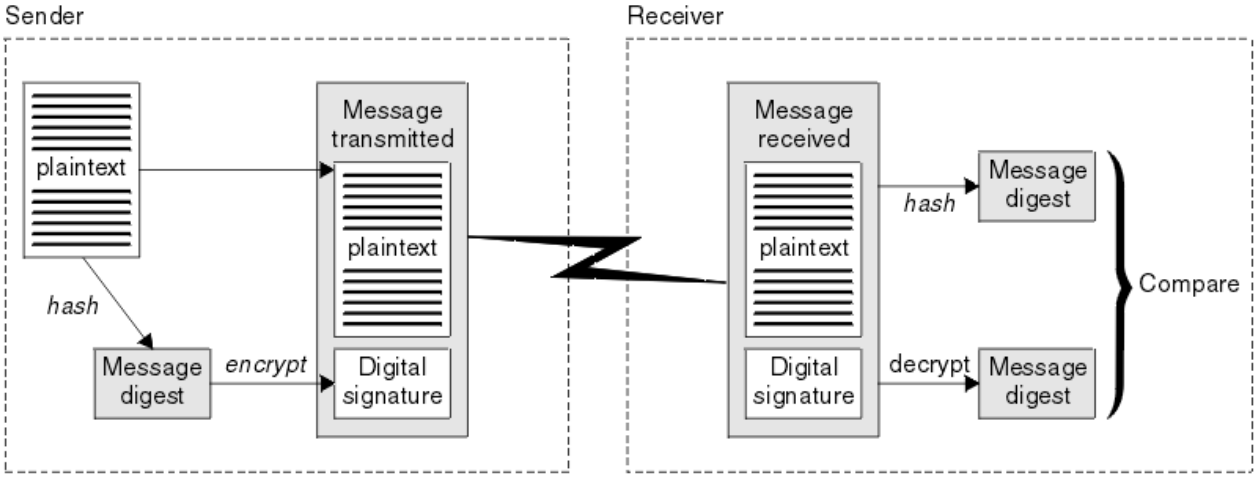
Digitální podpis je vytvořen šifrováním reprezentace zprávy. Šifrování používá soukromý klíč podepsané osoby a v zájmu efektivity obvykle pracuje na kódu digest zprávy spíše než na samotném zprávě.

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 19 .



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 zabezpečení, včetně šifrování dat. Národní ústav pro standardy a technologie (NIST) je důležitým subjektem, který se zabývá IT systémy a bezpečností. NIST produkuje doporučení a standardy, včetně standardů FIPS (Federal Information Processing Standards).

Významný jeden z těchto standardů je standard FIPS 140-2, který vyžaduje použití silných šifrovacích algoritmů. FIPS 140-2 také uvádí požadavky pro algoritmy hašování, které mají být použity k ochraně paketů před úpravou při přenosu.

Produkt IBM WebSphere MQ poskytuje podporu FIPS 140-2, byla-li konfigurována tak, aby to bylo možné provést.

V průběhu času analytici vyvíjejí útoky proti existujícím algoritmům šifrování a hašovací funkce. Jsou přijaty nové algoritmy, které odolávají těmto útokům. Standard FIPS 140-2 je pravidelně aktualizován, aby zohledněný tyto změny zohledněný.

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 kompatibilní se sadou Suite B pro použití se TLS verze 1.2. Je-li konfigurována pro kompatibilní operaci Suite B, bude použita pouze omezená sada šifrovacích algoritmů uvedených výše.
2. Přechodný profil pro použití s TLS verze 1.0 nebo TLS verze 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.

V systémech Windows, UNIX a Linux lze WebSphere MQnakonfigurovat tak, aby vyhovovalo profilu TLS 1.2 standardu Suite B, ale přechodný profil Suite B nepodporuje. Další informace uvádí téma “Šifrování NSA Suite B v produktu IBM WebSphere MQ” na stránce 30.

Související informace

“Federální standardy zpracování informací” na stránce 19
Americká vláda poskytuje technické poradenství v oblasti IT systémů a zabezpečení, včetně šifrování dat. Národní ústav pro standardy a technologie (NIST) je důležitým subjektem, který se zabývá IT systémy a bezpečností. NIST produkuje doporučení a standardy, včetně standardů FIPS (Federal Information Processing Standards).

IBM WebSphere MQ mechanismy zabezpečení

Tato kolekce témat vysvětluje, jak můžete implementovat různé koncepce zabezpečení v produktu IBM WebSphere MQ.

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

Identifikace a ověření v produktu IBM WebSphere MQ

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

Zde je několik příkladů identifikace a ověření v prostředí produktu IBM WebSphere 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 5

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 WebSphere MQ

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

Zde je několik příkladů autorizace v prostředí IBM WebSphere MQ :

- Povolení vydávat příkazy pro správu prostředků IBM WebSphere MQ pouze autorizovaným administrátorovi.
- 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 48 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 WebSphere MQ

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

Zde je několik příkladů auditování v prostředí IBM WebSphere 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 WebSphere MQ

Důvěryhodnost v produktu IBM WebSphere MQ můžete implementovat pomocí šifrování zpráv.

Zde je několik příkladů toho, jak lze zajistit důvěrnost v prostředí produktu IBM WebSphere MQ :

- Jakmile odesílající agent MCA obdrží zprávu z přenosové fronty, produkt IBM WebSphere MQ použije zabezpečení SSL nebo TLS k zašifrování zprávy před tím, než je odeslán 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 WebSphere MQ považovány za dostatečné pro ochranu jejich obsahu před neoprávněným zveřejněním. Avšak pro vyšší úroveň zabezpečení můžete použít produkt IBM WebSphere MQ Advanced Message Security k zašifrování zpráv uložených ve frontách.

Související pojmy

“Důvěrnost” na stránce 7

Služba *confidentiality* chrání citlivé informace před neoprávněným zveřejněním.

Integrita dat v produktu IBM WebSphere MQ

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

Zde je několik příkladů, jak lze zajistit integritu dat v prostředí produktu IBM WebSphere MQ :

- Protokol SSL nebo TLS můžete použít k zjištění, zda byl obsah zprávy během přenosu po síti úmyslně změněn. V protokolu SSL a TLS poskytuje algoritmus kódu digest zprávy detekce upravených zpráv při přenosu. Všechny IBM WebSphere MQ CipherSpecs poskytují algoritmus kódu digest zprávy, s výjimkou typu TLS_RSA_WITH_NULL_NULL, který neposkytuje integritu dat zprávy.
- Zatímco zprávy jsou uloženy v lokální frontě, mohou být mechanizmy řízení přístupu poskytované produktem IBM WebSphere MQ považovány za dostatečné pro zabránění záměrné úpravě obsahu zpráv. Avšak pro vyšší úroveň zabezpečení můžete pomocí produktu IBM WebSphere MQ Advanced Message Security zjistit, zda obsah zprávy byl mezi časem vložení zprávy do fronty a času načtenou z fronty úmyslně změněn.

Související pojmy

“Integrita dat” na stránce 7

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

Šifrování v produktu IBM WebSphere MQ

IBM WebSphere MQ poskytuje šifrování pomocí protokolů SSL (Secure sockets Layer) a TLS (Transport Security Layer).

Další informace viz “Protokoly zabezpečení v produktu IBM WebSphere MQ” na stránce 22.

Související pojmy

“Koncepce šifrování” na stránce 7

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

Protokoly zabezpečení v produktu IBM WebSphere MQ

IBM WebSphere MQ podporuje protokol TLS (Transport Layer Security) i protokol SSL (Secure Sockets Layer) k zajištění zabezpečení na úrovni linky pro kanály zpráv a kanály MQI.

Kanály zpráv a kanály MQI mohou používat protokol SSL nebo TLS k zajištění zabezpečení na úrovni odkazů.Volající agent MCA je klient SSL nebo TLS a modul MCA odezvy je serverem SSL nebo TLS. Produkt WebSphere MQ podporuje verzi 3.0 protokolu SSL a verzi 1.0 a verzi 1.2 protokolu TLS (Transport Layer Security). Určíte šifrovací algoritmy, které používá protokol SSL nebo protokol dodáním CipherSpec jako součásti definice kanálu.

Na každém konci kanálu zpráv a na konci serveru kanálu MQI pracuje agent MCA v zastoupení správce front, k němuž je připojen. Při navázání komunikace přes SSL nebo TLS odesílá agent MCA digitální certifikát správce front svému partnerovi MCA na druhém konci kanálu. Kód WebSphere MQ na straně klienta kanálu MQI zpracovává jménem uživatele klientské aplikace produktu WebSphere MQ . Během navázání komunikace přes zabezpečení SSL nebo TLS odesílá kód produktu WebSphere MQ digitální certifikát uživatele do agenta MCA na konci kanálu MQI.

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

Digitální certifikáty jsou uloženy v *úložišti klíčů* . The queue manager attribute *SSLKeyRepository* specifies the location of the key repository that holds the queue manager's digital certificate. On a WebSphere MQ client system, the MQSSLKEYR environment variable specifies the location of the key repository that holds the user's digital certificate. Alternativně může aplikace klienta WebSphere MQ určit své umístění v poli

KeyRepository ve struktuře voleb konfigurace SSL a TLS, MQSCO, na volání MQCONNX. Další informace o klíčových úložištích a o tom, jak určit, kde jsou umístěny, najdete v souvisejících tématech.

Související pojmy

"Kryptografické protokoly zabezpečení: SSL a 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). Produkt IBM WebSphere MQ podporuje zabezpečení SSL i TLS.

Podpora produktu IBM WebSphere MQ pro zabezpečení SSL a TLS

IBM WebSphere MQ podporuje protokol Secure Sockets Layer (SSL) a protokol TLS (Transport Layer Security).

Další informace o protokolech SSL a TLS naleznete v souvisejících informacích.

Produkt IBM WebSphere MQ poskytuje následující podporu pro SSL verze 3.0 a TLS 1.0 a TLS 1.2:

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

Systémy UNIX, Linux, and Windowsa HP Integrity NonStop Server
Pro systémy UNIX, Linux, and Windowsa HP Integrity NonStop Server je podpora zabezpečení SSL a TLS nainstalována s produktem IBM WebSphere MQ.

Informace o předpokladech pro podporu SSL a TLS produktu IBM WebSphere MQ naleznete v tématu Systémové požadavky pro produkt IBM WebSphere MQ.

Úložiště klíčů SSL nebo TLS
Vzájemně ověřené připojení SSL nebo TLS vyžaduje na každém konci připojení úložiště klíčů (které mohou být známy pod různými názvy na různých platformách). 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. Specifické názvy úložišť použité na platformách a prostředích, které podporují SSL a TLS, jsou:

Java a JMS	úložiště klíčů a důvěryhodné úložiště
 Systémy Windows , UNIX and Linux	soubor databáze klíčů

Další informace viz "digitální certifikáty" na stránce 9 a "Koncepce zabezpečení SSL (Secure Sockets Layer) a TLS (Transport Layer Security)" na stránce 14.

Vzájemně ověřené připojení SSL nebo TLS vyžaduje úložiště klíčů na každém konci připojení. Úložiště klíčů může obsahovat:

- 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. Přidružte samostatný osobní certifikát ke každému správci front nebo klientovi WebSphere MQ MQI. Osobní certifikáty jsou nezbytné pro klienta SSL nebo TLS, je-li vyžadováno 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 WebSphere MQ" na stránce 24.

Umístění úložiště klíčů závisí na platformě, kterou používáte:

systémy Windows, UNIX and Linux

Na systémech Windowsje klíčovým úložištěm klíčů UNIX and Linux soubor databáze klíčů. Název souboru databáze klíčů musí mít příponu `.kdb`. Příklad: V systému UNIX and Linuxje výchozí soubor databáze klíčů pro správce front `QM1` `/var/mqm/qmgrs/QM1/ssl/key.kdb` . Je-li produkt IBM WebSphere MQ nainstalován ve výchozím umístění, je ekvivalentní cesta v systému Windows `C:\Program Files\IBM\WebSphere MQ\Qmgrs\QM1\ssl\key.kdb`.

Na systémech Windows , UNIX and Linux má každý soubor klíčů databáze 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: Na systémech Windows, UNIX and Linux , mohou šifrovací hardwarové karty PKCS #11 obsahovat certifikáty a klíče, které jsou jinak uloženy v souboru databáze klíčů. Jsou-li certifikáty a klíče uchovávány na kartách PKCS #11 , produkt WebSphere MQ stále vyžaduje přístup k souboru databáze klíčů a k souboru pro uložení hesla.

V systémech Windows a UNIX databáze klíčů obsahuje také soukromý klíč pro osobní certifikát přidružený ke správci front nebo ke klientovi WebSphere MQ MQI.

Ochrana úložišť klíčů IBM WebSphere MQ
Úložiště klíčů pro IBM WebSphere 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 WebSphere 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.

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 aktualizovat také pomocí příkazů PCF nebo Průzkumníka produktu WebSphere MQ . Další informace naleznete v tématu Příkaz MQCMD_REFRESH_SECURITY a v tématu *Aktualizace zabezpečení SSL nebo TLS* v sekci WebSphere MQ Explorer v této dokumentaci produktu.

Související pojmy
“Aktualizace pohledu klienta na obsah úložiště klíčů SSL a nastavení zabezpečení SSL” na stránce 24
Chcete-li aktualizovat klientskou aplikaci s aktualizovaným obsahem úložiště klíčů, musíte aplikaci klienta zastavit a restartovat.

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

Zabezpečení klienta WebSphere MQ nelze obnovit; pro více informací neexistuje ekvivalent k příkazu REFRESH SECURITY TYPE (SSL) pro klienty (viz REFRESH SECURITY).

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 24
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).

Federální standardy zpracování informací (FIPS)
Toto téma představuje produkt Federal Information Processing Standards (FIPS) Cryptographic Validation Program of the US National Institute of Standards and Technology and the cryptographic functions which can be used on SSL nebo TLS channels, for Windows, UNIX and Linuxa z/OS systems.

Shoda s FIPS 140-2 připojení IBM WebSphere MQ zabezpečení SSL nebo TLS na systémech UNIX, Linuxa Windows se nachází zde "Standard FIPS (Federal Information Processing Standards) pro systémy UNIX, Linuxa Windows" na stránce 25.

Je-li přítomen kryptografický hardware, mohou být kryptografické moduly používané produktem IBM WebSphere MQ konfigurovány jako šifrovací moduly, které jsou poskytovány výrobcem hardwaru. Je-li toto provedeno, konfigurace bude vyhovovat pouze FIPS, pokud jsou tyto šifrovací moduly certifikovány FIPS-.

V průběhu času se standardy FIPS (Federal Information Processing Standards) aktualizují, aby odrážely nové útoky na šifrovací algoritmy a protokoly. Například některé CipherSpecs mohou přestat být certifikovány FIPS. Když se takové změny vyskytnou, produkt IBM WebSphere MQ se také aktualizuje, aby implementoval nejnovější standard. V důsledku toho může dojít po provedení údržby ke změnám chování.

Související pojmy

"Určení, že pro běhové prostředí klienta MQI je použit pouze certifikovaný standard FIPS CipherSpecs" na stránce 106
Vytvořte svá úložiště klíčů pomocí softwaru vyhovujícího standardu FIPS a poté zadejte, že kanál musí používat certifikovanou FIPS CipherSpecs.

"Použití iKeyman, iKeycmd, runmqakm a runmqckm" na stránce 111
V systémech UNIX, Linux a Windows spravujte klíče a digitální certifikáty pomocí rozhraní GUI iKeyman nebo z příkazového řádku pomocí příkazu iKeycmd nebo runmqakm.

Související úlohy

Povolení zabezpečení SSL v třídách WebSphere MQ pro jazyk Java

Použití zabezpečení SSL (Secure Sockets Layer) s třídami produktu WebSphere MQ pro platformu JMS

Související odkazy

Vlastnosti SSL pro objekty platformy JMS

Související informace

"Federální standardy zpracování informací" na stránce 19
Americká vláda poskytuje technické poradenství v oblasti IT systémů a zabezpečení, včetně šifrování dat. Národní ústav pro standardy a technologie (NIST) je důležitým subjektem, který se zabývá IT systémy a bezpečností. NIST produkuje doporučení a standardy, včetně standardů FIPS (Federal Information Processing Standards).

Standard FIPS (Federal Information Processing Standards) pro systémy UNIX, Linuxa Windows
Je-li vyžadováno šifrování v kanálu SSL nebo TLS v systémech Windows, UNIX and Linux používá produkt WebSphere MQ šifrovací balík s názvem IBM Crypto for C (ICC). Na platformách Windows, UNIX and Linux 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.

Shoda standardu FIPS 140-2 pro připojení WebSphere MQ SSL nebo TLS v systémech Windows, UNIX and Linux je následující:

- Pro všechny kanály zpráv IBM WebSphere 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 klienta IBM WebSphere MQ MQI 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 MQI.
  - Všechna úložiště klíčů byla vytvořena a byla s nimi manipulována pouze pomocí softwaru vyhovujícího standardu FIPS, jako např. **runmqakm** s volbou `-fips` .
- Pro třídy IBM WebSphere MQ pro aplikace Java používající režim klienta používá připojení implementace SSL a TLS prostředí JRE a vyhovuje standardu FIPS, pokud jsou splněny následující podmínky:
  - Prostředí Java Runtime Environment použité ke spuštění aplikace vyhovuje standardu FIPS na nainstalované verzi operačního systému a hardwarové architektuře.
  - Uvedli jste, že se má použít pouze šifrování s certifikací FIPS, jak je popsáno v souvisejícím tématu pro klienta Java.
  - Všechna úložiště klíčů byla vytvořena a byla s nimi manipulována pouze pomocí softwaru vyhovujícího standardu FIPS, jako např. **runmqakm** s volbou `-fips` .
- Pro třídy IBM WebSphere MQ pro aplikace JMS používající režim klienta používá připojení implementace SSL a TLS prostředí JRE a vyhovuje standardu FIPS, pokud jsou splněny následující podmínky:
  - Prostředí Java Runtime Environment použité ke spuštění aplikace vyhovuje standardu FIPS na nainstalované verzi operačního systému a hardwarové architektuře.
  - Určili jste, že se má použít pouze šifrování s certifikací FIPS, jak je popsáno v souvisejícím tématu pro klienta 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 se má použít pouze šifrování s certifikací FIPS, jak je popsáno v souvisejícím tématu pro klienta .NET.
  - Všechna úložiště klíčů byla vytvořena a byla s nimi manipulována pouze pomocí softwaru vyhovujícího standardu FIPS, 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 k rozhraní 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 AIX, Linux, HP-UX, Solaris, Windowsa z/OS mají certifikaci FIPS 140-2, kromě toho, jak je uvedeno v souboru README, který je součástí každé opravné sady nebo aktualizační sady.

Pro připojení SSL a 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 WebSphere 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.

Poznámka: 32bitoví klienti Solaris x86 s protokolem SSL a TLS, nakonfigurovaní pro operace dle standardu FIPS 140-2, selžou, budete-li je provozovat na systémech Intel. K tomuto selhání dochází, protože soubor 32bitové knihovny GSKit-Crypto Solaris x86 vyhovující specifikaci FIPS 140-2 se do čipové sady Intel nenačte. V zasažených systémech se do protokolu chyb klienta nahlásí chyba AMQ9655. Tento problém vyřešíte tak, že vypnete kompatibilitu se specifikací FIPS 140-2, nebo znovu zkompilujete aplikaci klienta pro 64 bitů, protože 64bitový kód není dotčen.

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

Je-li produkt WebSphere MQ konfigurován tak, aby pracoval v souladu se standardem FIPS 140-2, jsou ve vztahu k specifikaci 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 WebSphere MQ neresetuje 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 219.

Produkt WebSphere MQ generuje klíče relace Triple DES, které jsou již v souladu s pravidly 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 pro běhové prostředí klienta MQI je použit pouze certifikovaný standard FIPS CipherSpecs” na stránce 106
Vytvořte svá úložiště klíčů pomocí softwaru vyhovujícího standardu FIPS a poté zadejte, že kanál musí používat certifikovanou FIPS CipherSpecs.

“Použití iKeyman, iKeycmd, runmqakm a runmqckm” na stránce 111
V systémech UNIX, Linux a Windows spravujte klíče a digitální certifikáty pomocí rozhraní GUI iKeyman nebo z příkazového řádku pomocí příkazu iKeycmd nebo runmqakm.

Související úlohy

Povolení zabezpečení SSL ve třídách WebSphere MQ pro jazyk Java

Použití zabezpečení SSL (Secure Sockets Layer) se třídami WebSphere MQ pro platformu JMS

Související odkazy

Vlastnosti SSL objektů JMS

Související informace

“Federální standardy zpracování informací” na stránce 19
Americká vláda poskytuje technické poradenství v oblasti IT systémů a zabezpečení, včetně šifrování dat. Národní ústav pro standardy a technologie (NIST) je důležitým subjektem, který se zabývá IT systémy a bezpečností. NIST produkuje doporučení a standardy, včetně standardů FIPS (Federal Information Processing Standards).

SSL a TLS v klientovi IBM WebSphere MQ MQI

Produkt IBM WebSphere MQ podporuje zabezpečení SSL a TLS na klientech. Použití SSL nebo TLS můžete přizpůsobit různými způsoby.

Produkt IBM WebSphere MQ poskytuje podporu zabezpečení SSL a TLS pro klienty IBM WebSphere MQ MQI v systémech Windows, UNIX and Linux . Používáte-li třídy produktu IBM WebSphere MQ for Java, projděte si téma Použití tříd WebSphere MQ pro jazyk Java a používáte-li třídy produktu IBM WebSphere MQ pro platformu JMS, přečtěte si téma Použití tříd produktu WebSphere MQ pro systém JMS. Zbývající část tohoto oddílu se nevztahuje na prostředí Java nebo JMS.

Můžete určit úložiště klíčů pro klienta IBM WebSphere MQ MQI buď s hodnotou MQSSLKEYR v konfiguračním souboru klienta IBM WebSphere MQ , nebo při volání aplikace MQCONNX. Existují tři možnosti určení, že kanál používá zabezpečení SSL:

- 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 zabezpečení SSL.

Můžete pokračovat ve spouštění stávajících aplikací klienta IBM WebSphere MQ MQI bez zabezpečení SSL, dokud nebude na druhém konci kanálu určena hodnota SSL.

Jsou-li na klientském počítači provedeny změny v obsahu úložiště klíčů SSL, umístění úložiště klíčů SSL, informací o ověření nebo šifrovacích hardwarových parametrů, je třeba ukončit všechna připojení SSL, aby se tyto změny projevily v kanálech připojení klienta, které aplikace používá pro připojení ke správci front. Po ukončení všech připojení restartujte kanály zabezpečení SSL. Všechny nové nastavení SSL se použijí. Tato nastavení jsou analogická k těm nastavením obnovených příkazem REFRESH SECURITY TYPE (SSL) v systémech správce front.

Je-li klient IBM WebSphere MQ MQI spuštěn v systému Windows, systém UNIX and Linux s kryptografickým hardwarem, tento hardware nakonfigurujete 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 zabezpečení SSL a FIPS jsou podporovány na klientech IBM WebSphere MQ MQI. Další informace naleznete v tématech “Resetování tajných klíčů SSL a TLS” na stránce 219 a “Standard FIPS (Federal Information Processing Standards) pro systémy UNIX, Linuxa Windows” na stránce 25.

Další informace o podpoře SSL pro klienty IBM WebSphere MQ MQI viz “Nastavení zabezpečení klienta IBM WebSphere MQ MQI” na stránce 105 .

Související úlohy

Konfigurace klienta pomocí konfiguračního souboru

Určení, že kanál MQI používá zabezpečení SSL

Má-li kanál MQI používat zabezpečení SSL, hodnota atributu *SSLCipherSpec* kanálu připojení klienta musí představovat název CipherSpec , který je podporován produktem IBM WebSphere 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 klienta WebSphere MQ MQI vydá volání MQCONNX, bude k ní vydáno 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 ve volání MQCONNX, bude tato definice použita přednostně pro všechny položky v tabulce definic kanálů klienta, k nimž může přistupovat klient WebSphere MQ .

Proměnnou prostředí MQSERVER nelze použít k poskytnutí definice kanálu na straně klienta kanálu MQI, který používá zabezpečení SSL.

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 položky CipherSpec pro klienta IBM WebSphere MQ MQI” na stránce 218
Existují tři možnosti zadání volby CipherSpec pro klienta IBM WebSphere MQ MQI.

CipherSpecs a CipherSuites v produktu IBM WebSphere MQ

Produkt IBM WebSphere MQ podporuje jak algoritmy SSL, tak TLS CipherSpecs, tak algoritmy RSA a Diffie-Hellman.

WebSphere MQ podporuje SSL V3 a TLS V1.0 a V1.2 CipherSpecs.

Produkt WebSphere MQ podporuje algoritmus výměny klíčů RSA a Diffie-Hellman a ověřovací algoritmy. Velikost klíče použitého během navázání komunikace přes zabezpečení SSL může záviset na použitém digitálním certifikátu, ale některé 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 18
Kryptografické bezpečnostní protokoly musí souhlasit s algoritmem používaným zabezpečeným připojením. CipherSpecs a CipherSuites definují specifické kombinace algoritmů.

Šifrování NSA Suite B v produktu IBM WebSphere MQ
Toto téma poskytuje informace o tom, jak nakonfigurovat produkt IBM WebSphere MQ na systémech Windows, Linuxa UNIX tak, aby vyhovoval profilu TLS 1.2 standardu Suite B.

V průběhu času se aktualizuje standard NSA Cryptography Suite B Standard tak, aby odrážel nové útoky na šifrovací algoritmy a protokoly. Například některé CipherSpecs mohou přestat být certifikovány Suite B. Když se takové změny vyskytnou, produkt IBM WebSphere MQ se také aktualizuje, aby implementoval nejnovější standard. V důsledku toho může dojít po provedení údržby ke změnám chování. Soubor Readme produktu IBM WebSphere MQ Version 7.5 uvádí verzi sady Suite B, která je vynucena jednotlivými úrovněmi údržby produktu. Pokud nakonfigurujete produkt IBM WebSphere MQ k vynucení kompatibility s Suite B, vždy při plánování údržby v souboru Readme konzultujte soubor README (viz IBM MQ, WebSphere MQa MQSeries produktu READMEs).

V systémech Windows, UNIXa Linux lze IBM WebSphere MQ nakonfigurovat tak, aby vyhovovalo profilu TLS 1.2 standardu Suite B na úrovních zabezpečení uvedených v tabulce 1.

Tabulka 1. Úrovně zabezpečení Suite B s povolenými povolenými algoritmy CipherSpecs a digitálním podpisem

Úroveň zabezpečení	**Povolené specifikace 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
Oba[1]	ECDHE_ECDSA_AES_128_GCM_SHA256 ECDHE_ECDSA_AES_256_GCM_SHA384	ECDSA s SHA-256 ECDSA s SHA-384

1. Je možné souběžně nakonfigurovat jak 128bitové, tak 192bitové úrovně zabezpečení. Vzhledem k tomu, že konfigurace Suite B určuje minimální přijatelné šifrovací algoritmy, je konfigurace obou úrovní zabezpečení ekvivalentní nastavení pouze 128bitové úrovně zabezpečení. Šifrovací algoritmy 192bitové úrovně zabezpečení jsou silnější než minimální požadované pro 128bitovou úroveň zabezpečení, takže jsou povoleny pro 128bitovou úroveň zabezpečení i v případě, že není povolena 192bitová úroveň zabezpečení.

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

Konformace CipherSpec pro sadu Suite B

Ačkoli výchozí chování produktu IBM WebSphere MQ není v souladu se standardem Suite B, produkt IBM WebSphere MQ může být nakonfigurován tak, aby vyhovoval oběma úrovním zabezpečení na systémech Windows, UNIX a Linux . Po úspěšné konfiguraci produktu IBM WebSphere MQ pro použití Suite B se každý pokus o spuštění odchozího kanálu pomocí sady CipherSpec , která neodpovídá standardu Suite B, za následek chyby AMQ9282. Tato aktivita také má za následek vrácení kódu příčiny MQRC_CIPHER_SPEC_NOT_SUITE_Bklientem MQI. Podobně se při pokusu o spuštění příchozího kanálu pomocí specifikace CipherSpec , která neodpovídá konfiguraci sady Suite B, došlo k chybě v chybě AMQ9616.

Další informace o produktu WebSphere MQ CipherSpecsviz “Určení CipherSpecs” na stránce 213

Suite B a digitální certifikáty

Suite B omezuje algoritmy digitálního podpisu, které lze použít pro podepisování digitálních certifikátů. Suite B také omezuje typ veřejného klíče, který mohou certifikáty obsahovat. Proto musí být produkt WebSphere MQ nakonfigurován tak, aby používal certifikáty, jejichž algoritmus digitálního podpisu a typ veřejného klíče je povolen pro konfigurovanou úroveň zabezpečení Suite B vzdáleného partnera. Digitální certifikáty, které nevyhovují požadavkům na úroveň zabezpečení, jsou odmítnuty a připojení selže s chybou AMQ9633 nebo AMQ9285.

Pro 128bitovou úroveň zabezpečení Suite B je požadován veřejný klíč certifikátu k použití buď eliptické křivky NIST P-256 nebo eliptické křivky NIST P-384 a k podepsání buď s eliptickou křivkou NIST P-256 nebo eliptickou křivkou NIST P-384 . Na úrovni zabezpečení 192 bitů Suite B je požadován veřejný klíč subjektu certifikátu pro použití eliptické křivky NIST P-384 a k podpisu s eliptickou křivkou NIST P-384 .

Chcete-li získat certifikát vhodný pro kompatibilní operaci Suite B, použijte příkaz **runmqakm** a uveďte parametr **-sig_alg** , abyste požádali o vhodný algoritmus digitálního podpisu. Hodnoty parametrů EC_ecdsa_with_SHA256 a EC_ecdsa_with_SHA384 **-sig_alg** odpovídají hodnotám eliptických křivek, které jsou podepsány povolenými algoritmy digitálního podpisu Suite B.

Další informace o příkazu **runmqakm** naleznete v volbách runmqckm a runmqakm.

Poznámka: Nástroje **iKeycmd** a **iKeyman** nepodporují vytváření digitálních certifikátů pro kompatibilní operaci Suite B.

Vytvoření a vyžádání digitálních certifikátů

Chcete-li vytvořit certifikát podepsaný držitelem pro testování Suite B, prohlédněte si téma “Vytvoření osobního certifikátu s automatickým podpisem na systémech UNIX, Linux, and Windows” na stránce 119

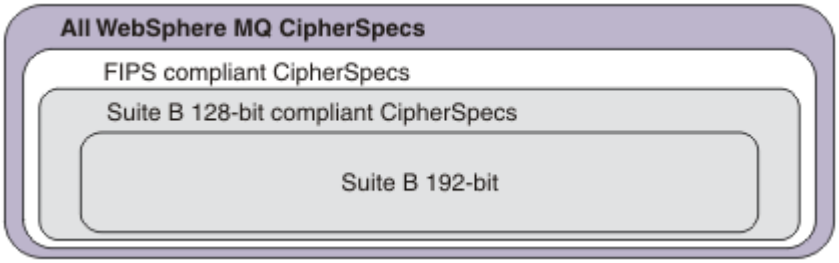
Chcete-li požádat o digitální certifikát podepsaný CA pro provozní použití Suite B, prohlédněte si téma “Požádání o osobní certifikát na systémech UNIX, Linux, and Windows” na stránce 121.

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

FIPS 140-2 a Suite B

Standard Suite B je koncepčně podobný standardu FIPS 140-2, neboť omezuje sadu povolených šifrovacích algoritmů tak, aby byla zajištěna zajištěná úroveň zabezpečení. Aktuálně podporovaná sada Suite B CipherSpecs lze použít, je-li IBM WebSphere MQ konfigurováno pro operaci vyhovující FIPS 140-2. Proto je možné produkt WebSphere MQ nakonfigurovat současně pro shodu FIPS a Suite B současně, v tom případě se použijí obě sady omezení.

Následující diagram ilustruje vztah mezi těmito dílčími sadami:



Konfigurace produktu WebSphere MQ pro kompatibilní operaci sady Suite B

Informace o tom, jak nakonfigurovat produkt IBM WebSphere MQ v systému Windows, UNIX a Linux pro kompatibilní operaci Suite B naleznete v tématu “Konfigurace produktu IBM WebSphere MQ pro sadu Suite B” na stránce 32.

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

Související pojmy

“Určení, že pro běhové prostředí klienta MQI je použit pouze certifikovaný standard FIPS CipherSpecs” na stránce 106
Vytvořte svá úložiště klíčů pomocí softwaru vyhovujícího standardu FIPS a poté zadejte, že kanál musí používat certifikovanou FIPS CipherSpecs.

Konfigurace produktu IBM WebSphere MQ pro sadu Suite B
Produkt IBM WebSphere MQ lze nakonfigurovat tak, aby pracoval v souladu se standardem NSA Suite B v systémech UNIX, Linux, and Windows .

Sada B omezuje sadu povolených šifrovacích algoritmů tak, aby byla zajištěna zajištěná úroveň zabezpečení. IBM WebSphere MQ může být konfigurován tak, aby fungoval v souladu se sadou Suite B, aby byla zajištěna vyšší úroveň zabezpečení. Další informace o Suite B najdete v tématu “Národní bezpečnostní agentura (NSA) Suite B Kryptografie” na stránce 19. Další informace o konfiguraci sady Suite B a jejím vlivu na kanály SSL a TLS naleznete v tématu “Šifrování NSA Suite B v produktu IBM WebSphere MQ” na stránce 30.

Správce front

Pro správce front použijte příkaz **ALTER QMGR** s parametrem **SUITEB** k nastavení hodnot vhodných pro požadovanou úroveň zabezpečení. Další informace viz ALTER QMGR.

Příkaz PCF **MQCMD_CHANGE_Q_MGR** s parametrem **MQIA_SUITE_B_STRENGTH** můžete také použít ke konfiguraci správce front pro kompatibilní operaci Suite B.

Klient MQI

Při výchozím nastavení klienti MQI nevynucují shodu Suite B. Klienta MQI pro shodu sady Suite B můžete povolit provedením jedné z níže uvedených voleb:

1. Nastavením pole **EncryptionPolicySuiteB** ve struktuře MQSCO na volání MQCONNX na jednu nebo více níže uvedených hodnot:
   - MQ_SUITE_B_NONE
   - MQ_SUITE_B_128_BIT
   - MQ_SUITE_B_192_BIT

   Použití proměnné MQ_SUITE_B_NONE s jakoukoli jinou hodnotou je neplatné.
2. Nastavením proměnné prostředí MQSUITEB na jednu nebo více níže uvedených hodnot:
   - ŽÁDNÉ
   - 128_BIT
   - 192_BIT

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

   Více hodnot lze zadat pomocí seznamu odděleného čárkami. Použití hodnoty NONE s jakoukoli jinou hodnotou je neplatné.

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

Podrobné informace o struktuře MQSCO naleznete v tématu Volby konfigurace MQSCO-SSL.

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

Další informace o použití proměnné prostředí MQSUITEB naleznete v tématu Proměnné prostředí.

.NET

Pro nespravované klienty .NET je vlastnost **MQC.ENCRYPTION_POLICY_SUITE_B** označuje typ zabezpečení Suite B, který je požadován.

Informace o použití Suite B ve třídách IBM WebSphere MQ pro .NET najdete v tématu Třída MQEnvironment .NET.

Zásady ověření platnosti certifikátu v produktu IBM WebSphere 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 zásada ověření platnosti certifikátu závisí na komponentě JSSE prostředí JRE (Java Runtime Environment). Další informace o zásadě ověření platnosti certifikátu naleznete v dokumentaci k vašemu prostředí JRE.
- Pro systémy UNIX, 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 systémech UNIX, Linux, and Windows , viz “Konfigurace zásad ověření platnosti certifikátu v produktu IBM WebSphere MQ” na stránce 33. Další informace o rozdílech mezi zásadami základního a standardního ověření certifikátu naleznete v tématu Ověření platnosti certifikátu a návrh zásad důvěryhodnosti v systémech UNIX, Linux a Windows .

Konfigurace zásad ověření platnosti certifikátu v produktu IBM WebSphere MQ
Můžete určit, která zásada ověření certifikátu SSL/TLS se použije k ověření platnosti digitálních certifikátů přijatých ze vzdálených partnerských systémů čtyřmi způsoby.

Na správci front lze zásadu ověření certifikátu nastavit následujícími způsoby:

- Použití atributu správce front *CERTVPOL*. Další informace o nastavení tohoto atributu naleznete v tématu ALTER QMGR .

Na straně klienta existuje několik metod, které lze použít k nastavení zásady ověření platnosti certifikátu. Je-li pro nastavení zásady použita více než jedna metoda, použije klient nastavení v následujícím pořadí priority:

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

Další informace o zásadách ověření platnosti certifikátů viz “Zásady ověření platnosti certifikátu v produktu IBM WebSphere MQ” na stránce 33.

Digitální certifikáty a kompatibilita CipherSpec v produktu IBM WebSphere MQ
Toto téma poskytuje informace o tom, jak vybrat příslušné CipherSpecs a digitální certifikáty pro svou strategii zabezpečení, a to tak, že nastiňují vztah mezi CipherSpecs a digitálními certifikáty v produktu IBM WebSphere MQ.

V předchozích vydáních produktu IBM WebSphere MQpoužívali všechny podporované SSL a TLS CipherSpecs algoritmus RSA pro digitální podpisy a klíčovou smlouvu. Všechny podporované typy digitálního certifikátu byly kompatibilní se všemi podporovanými CipherSpecs, takže bylo možné změnit CipherSpec pro každý kanál, aniž by bylo nutné měnit digitální certifikáty.

V produktu IBM WebSphere MQ v7.5 lze použít pouze podmnožinu podporovaných CipherSpecs se všemi podporovanými typy digitálního certifikátu. Je proto nezbytné zvolit příslušnou CipherSpec pro váš digitální certifikát. Podobně platí, že pokud zásady zabezpečení vaší organizace vyžadují, abyste použili konkrétní CipherSpec , musíte pro tuto CipherSpeczískat příslušný digitální certifikát.

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 považován za slabý mnoha kryptografickými analytiky a jeho použití je obecně nevhodné. Chcete-li použít novější verzi specifikace CipherSpecs na základě protokolu TLS 1.2 , zajistěte, aby digitální certifikáty nepoužívaly algoritmus MD5 ve svých digitálních podpisech. Starší CipherSpecs , které používají protokoly SSL 3.0 a TLS 1.0 , nejsou předmětem tohoto omezení a mohou nadále používat certifikáty s digitálním podpisem 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 označení certifikátu algoritmu digitálního podpisu, který potřebujete zobrazit.

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

Provedení příkazu **runmqakm** vytvoří výstup zobrazující použití zadaného podpisového algoritmu:

```
Label : ibmwebspheremqexample
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` udává, že je použit algoritmus `MD5WithRSASignature` . Tento algoritmus je založen na MD5 , takže tento digitální certifikát nelze použít s TLS 1.2 CipherSpecs.

Interoperabilita Eliptické křivky a RSA CipherSpecs

Ne všechny CipherSpecs lze použít se všemi digitálními certifikáty. Jsou zde tři typy CipherSpecoznačené předponou názvu CipherSpec . Každý typ CipherSpec klade různá omezení na typ digitálního certifikátu, který může být použit. Tato omezení se vztahují na všechna připojení SSL a TLS produktu WebSphere MQ , ale jsou zvláště důležitá pro uživatele šifrování Elliptic Curve.

Vztahy mezi CipherSpecs a digitálními certifikáty jsou shrnuty v následující tabulce:

Tabulka 2. Vztahy mezi CipherSpecs a digitálními certifikáty

Typ	Předpona názvu CipherSpec	Popis	Požadovaný typ veřejného klíče	Algoritmus šifrování digitálního podpisu	Metoda stanovení 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 Elliptic Curve.	RSA	RSA	ECDHE
3	(Všechny ostatní)	CipherSpecs , které používají veřejné klíče RSA a algoritmy digitálního podpisu RSA.	RSA	RSA	RSA

Poznámka: Typ 1 a 2 CipherSpecs jsou podporovány pouze správci front WebSphere MQ a klienty MQI na platformách UNIX, Linux, and Windows .

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

Algoritmus šifrování digitálního podpisu odkazuje na šifrovací algoritmus použitý k ověření partnera. Šifrovací algoritmus se používá spolu s algoritmem přepočtu klíče, jako je MD5, SHA-1 nebo SHA-256 k výpočtu digitálního podpisu. Jsou zde různé algoritmy digitálního podpisu, které lze použít, například "RSA with MD5" nebo "ECDSA with SHA-256". V tabulce se ECDSA odkazuje na sadu algoritmů digitálního podpisu, které používají ECDSA; RSA se odkazuje na sadu algoritmů digitálního podpisu, které používají RSA. Může být použit libovolný podporovaný algoritmus digitálního podpisu v sadě, je-li založen na uvedeném šifrovacím algoritmu.

Typ 1 CipherSpecs vyžaduje, aby osobní certifikát měl veřejný klíč Elliptic Curve. Jsou-li použity tyto specifikace CipherSpecs , použije se ke zřízení tajného klíče pro připojení klávesová dohoda Elliptic Curve Diffie Hellman Ephemeral.

Typ 2 CipherSpecs vyžaduje, aby osobní certifikát měl veřejný klíč RSA. Jsou-li použity tyto specifikace CipherSpecs , použije se ke zřízení tajného klíče pro připojení klávesová dohoda Elliptic Curve Diffie Hellman Ephemeral.

Typ 3 CipherSpecs vyžaduje, aby osobní certifikát měl veřejný klíč RSA. Jsou-li použity tyto specifikace CipherSpecs , je použita výměna klíče RSA k vytvoření tajného klíče pro připojení.

Tento seznam omezení není vyčerpávající: v závislosti na konfiguraci mohou existovat další omezení, která mohou dále ovlivnit schopnost spolupráce. Je-li například produkt WebSphere MQ konfigurován tak, aby vyhovoval standardům FIPS 140-2 nebo NSA Suite B, omezí se tím také rozsah přípustných konfigurací. Další informace naleznete v následující sekci.

Správce front produktu WebSphere MQ může použít pouze jeden osobní certifikát k identifikaci sebe sama. To znamená, že všechny kanály ve správci front budou používat stejný digitální certifikát, a proto každý správce front může v daném okamžiku používat pouze jeden typ CipherSpec . Podobně může klientská aplikace produktu WebSphere MQ používat pouze jeden osobní certifikát k identifikaci sebe sama. To znamená, že všechna připojení SSL a TLS v rámci jednoho procesu aplikace budou používat stejný digitální certifikát, a proto může každý proces aplikace klienta používat vždy pouze jeden typ CipherSpec .

Tři typy CipherSpec nespolupracují přímo: jedná se o omezení aktuálních standardů SSL a TLS. Předpokládejme například, že jste zvolili použití ECDHE_ECDSA_AES_128_CBC_SHA256 CipherSpec pro přijímací kanál s názvem TO.QM1 ve správci front s názvem QM1. ECDHE_ECDSA_AES_128_CBC_SHA256 je typ 1 CipherSpec, takže QM1 musí mít osobní certifikát s klíčem Elliptic Curve a digitálního podpisu na bázi ECDSA. Všichni klienti a další správci front, kteří komunikují přímo s produktem QM1 , musí mít proto digitální certifikáty, které splňují požadavky typu 1 CipherSpec . Další kanály, které se připojují ke správci front QM1 , mohou používat jiné specifikace CipherSpecs (například ECDHE_ECDSA_3DES_EDE_CBC_SHA256), ale mohou použít pouze typ CipherSpecs typu 1 pro komunikaci s QM1.

Při plánování sítí WebSphere MQ pečlivě zvažte, které kanály vyžadují SSL nebo TLS, a ujistěte se, že všichni klienti a správci front, kteří potřebují spolupracovat, používají stejný typ CipherSpecs a odpovídající digitální certifikáty. Standardy IETF RFC 4492, RFC 5246 a RFC 6460 popisují podrobné použití volby Elliptic Curve CipherSpecs v TLS 1.2.

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 označení certifikátu, jehož algoritmus digitálního podpisu je třeba zobrazit.

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

```
Label : ibmwebspheremqexample
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 Algoritmus podpisu v tomto případě ukazuje, že algoritmus EC_ecdsa_with_SHA384 se používá: je založen na algoritmu ECDSA. Tento certifikát je proto vhodný pouze pro použití s typem 1 CipherSpecs.

Nástroj **iKeycmd (runmqckm)** můžete také použít se stejnými parametry. Grafické rozhraní produktu **iKeyman (strmqikm)** lze také použít k zobrazení algoritmů digitálního podpisu, pokud otevřete úložiště klíčů a poklepání na popisek certifikátu. Doporučuje se však používat nástroj **runmqakm** k zobrazení digitálních certifikátů, protože podporuje širší rozsah algoritmů.

Eliptická křivka CipherSpecs a NSA Suite B

Je-li produkt WebSphere MQ nakonfigurován tak, aby vyhovoval profilu TLS 1.2 standardu Suite B, jsou povoleny povolené algoritmy CipherSpecs a digitální podpisové algoritmy, jak je popsáno v tématu "Šifrování NSA Suite B v produktu IBM WebSphere MQ" na stránce 30. Navíc je rozsah přijatelných klíčů Elliptic Curve zmenšen v závislosti na konfigurovaných úrovních zabezpečení.

Na úrovni zabezpečení 128 bitů Suite B se vyžaduje veřejný klíč subjektu certifikátu pro použití eliptické křivky NIST P-256 nebo NIST P-384 a k podepsání buď s eliptickou křivkou NIST P-256 nebo s eliptickou křivkou NIST P-384 . Příkaz **runmqakm** lze použít k vyžádání digitálních certifikátů pro tuto úroveň zabezpečení pomocí parametru -sig_alg příkazu EC_ecdsa_with_SHA256nebo EC_ecdsa_with_SHA384.

Na úrovni zabezpečení 192 bitů Suite B je veřejný klíč subjektu certifikátu vyžadován pro použití eliptické křivky NIST P-384 a k podpisu s eliptickou křivkou NIST P-384 . Příkaz **runmqakm** lze použít k požadavku na digitální certifikáty pro tuto úroveň zabezpečení pomocí parametru -sig_alg příkazu EC_ecdsa_with_SHA384.

Podporovaná NIST eliptický křivek je následující:

Tabulka 3. Podporované eliptické křivky NIST

Název křivky NIST FIPS 186-3	**Název křivky RFC 4492**	**Velikost klíče Elliptic Curve (bity)**
P-256	secp256r1	256
P-384	secp384r1	384
P-521	secp521r1	521

Poznámka: Eliptický křivku NIST P-521 nelze použít pro kompatibilní operaci Suite B.

Související pojmy

“Určení CipherSpecs” na stránce 213
Zadejte CipherSpec pomocí parametru **SSLCIPH** buď v příkazu **DEFINE CHANNEL** MQSC, nebo v příkazu **ALTER CHANNEL** MQSC.

“Určení, že pro běhové prostředí klienta MQI je použit pouze certifikovaný standard FIPS CipherSpecs” na stránce 106
Vytvořte svá úložiště klíčů pomocí softwaru vyhovujícího standardu FIPS a poté zadejte, že kanál musí používat certifikovanou FIPS CipherSpecs.

“Šifrování NSA Suite B v produktu IBM WebSphere MQ” na stránce 30
Toto téma poskytuje informace o tom, jak nakonfigurovat produkt IBM WebSphere MQ na systémech Windows, Linuxa UNIX tak, aby vyhovoval profilu TLS 1.2 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.

Hodnoty CipherSpec podporované v produktu IBM WebSphere MQ

Sada výchozích specifikací CipherSpecs povoluje pouze následující hodnoty:

TLS 1.0

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

TLS 1.2

- ECDHE_ECDSA_AES_128_CBC_SHA256
- ECDHE_ECDSA_AES_256_CBC_SHA384
- ECDHE_ECDSA_AES_128_GCM_SHA256
- ECDHE_ECDSA_AES_256_GCM_SHA384
- ECDHE_RSA_AES_128_CBC_SHA256
- ECDHE_RSA_AES_256_CBC_SHA384
- ECDHE_RSA_AES_128_GCM_SHA256
- ECDHE_RSA_AES_256_GCM_SHA384
- 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

Povolení zamítnutých CipherSpecs

Ve výchozím nastavení není povoleno určit zamítnutou položku CipherSpec v definici kanálu. Pokud se pokusíte zadat zamítnutou volbu CipherSpec, obdržíte ve správci front zprávu AMQ9788 v protokolu chyb.

Je možné, abyste znovu povolili zamítnuté CipherSpecs úpravou souboru `qm.ini` . V sekci SSL souboru `qm.ini` přidejte následující řádek:

```
SSL:
AllowWeakCipherSpec=Yes
```

Můžete také znovu povolit jednu nebo více zamítnutých CipherSpecs v běhovém prostředí na serveru nastavením proměnné prostředí *AMQ_SSL_WEAK_CIPHER_ENABLE* na libovolnou hodnotu. Tato proměnná prostředí povoluje CipherSpecs bez ohledu na hodnotu, která je uvedena v souboru `qm.ini` .

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 WebSphere 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 4. 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 ověření kanálu můžete vytvořit, upravit nebo odebrat pomocí příkazu MQSC **SET CHLAUTH** nebo 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 WebSphere MQ. Tyto adresy musí být dočasně blokovány, dokud nedojde k aktualizaci brány firewall. Tyto pokusy o připojení nemusí být přijímány ani z kanálů produktu WebSphere MQ , ale z jiných aplikací soketů, které jsou nesprávně nakonfigurovány pro cíl vašeho modulu listener produktu WebSphere 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 178.

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 180.

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 deklarovaný ID uživatele klienta” na stránce 182.

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 182.

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" na stránce 183.

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 183.

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 180.

Mapování ID uživatelů deklarovaných klientem na používaná ID uživatele

Chcete-li určit, že v případě použití konkrétního ID uživatele připojením z klienta WebSphere MQ MQI má být použit jiný zadaný atribut MCAUSER, nastavte záznam ověřování kanálu typu USERMAP. Mapování ID uživatele nepoužívá žádné zástupné znaky.

Příklad najdete v části "Mapování uživatelem deklarovaného ID uživatele na ID uživatele MCAUSER" na stránce 181.

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 181.

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 180.

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.

Pokud počet záznamů ověřování kanálu odpovídá názvu kanálu, adrese IP, názvu správce front či rozlišujícího názvu SSL nebo TLS, dojde k použití nejlepší shody. Nejlepší shoda bude určena následujícím způsobem.

- Název kanálu:
  - Nejlepší shodou je název bez zástupných znaků, například A.B.C.
  - Nejobecnější shodou je jedna hvězdička (*), které odpovídají všechny názvy kanálů.
  - Vzorec s hvězdičkou na pozici zcela vlevo je obecnější než vzorec, který má na pozici zcela vlevo definovanou hodnotu. Vzorec *.B.C je tedy obecnější než vzorec A.*.
  - Vzorec s hvězdičkou na druhé pozici je obecnější než vzorec, který má na druhé pozici definovanou hodnotu, což platí obdobně i pro všechny další pozice. Vzorec A.*.C je tedy obecnější než vzorec A.B.*
  - Pokud mají dva nebo více vzorů hvězdičku na stejné pozici, je obecnější vzorec, kde po hvězdičce následuje menší počet uzlů. Takže A. * obecnější než A.*.C.
- Adresa IP:
  - Nejlepší shodou je název bez zástupných znaků, například 192.0.2.6.
  - Nejobecnější shodou je jedna hvězdička (*), které odpovídají všechny názvy kanálů.

  - Vzorec s hvězdičkou na pozici zcela vlevo je obecnější než vzorec, který má na pozici zcela vlevo definovanou hodnotu. Vzorec *.0.2.6 je tedy obecnější než vzorec 192.*.
  - Vzorec s hvězdičkou na druhé pozici je obecnější než vzorec, který má na druhé pozici definovanou hodnotu, což platí obdobně i pro všechny další pozice. Vzorec 192.*.2.6 je tedy obecnější než vzorec 192.0.*.
  - Pokud mají dva nebo více vzorů hvězdičku na stejné pozici, je obecnější vzorec, kde po hvězdičce následuje menší počet uzlů. Takže 192 .* obecnější než 192.*.2.*.
  - 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.
- Název správce front:
  - Nejlepší shodou je název bez zástupných znaků, například 192.0.2.6.
  - Nejobecnější shodou je jedna hvězdička (*), které odpovídají všechny názvy kanálů.
  - Vzorec s hvězdičkou na pozici zcela vlevo je obecnější než vzorec, který má na pozici zcela vlevo definovanou hodnotu. Vzorec *QUEUEMANAGER je tedy obecnější než vzorec QUEUEMANAGER*.
  - Vzorec s hvězdičkou na druhé pozici je obecnější než vzorec, který má na druhé pozici definovanou hodnotu, což platí obdobně i pro všechny další pozice. Vzorec Q*MANAGER je tedy obecnější než vzorec QUEUE*.
  - Pokud mají dva nebo více vzorů hvězdičku na stejné pozici, je obecnější vzorec, kde po hvězdičce následuje menší počet znaků. Vzorec Q* je obecnější než vzorec Q*MGR.
- V případě rozlišujícího názvu SSL nebo TLS je pořadí přednosti podřetězců následující:

Tabulka 5. 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

Tabulka 5. Pořadí přednosti v podřetězcích (pokračování)		
Pořadí	**Podřetězec rozlišujícího názvu**	**Název**
9	O=	Organizace
10	STREET=	Ulice/první řádek adresy
99,99%	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 WebSphere 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 ověření 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 54
Tento oddíl pojednává o aspektech zabezpečení vzdáleného systému zpráv.

Zabezpečení zpráv v produktu IBM WebSphere MQ

Zabezpečení zpráv v infrastruktuře produktu IBM WebSphere MQ je poskytováno samostatně licencovanou komponentou IBM WebSphere MQ Advanced Message Security.

Produkt IBM WebSphere MQ Advanced Message Security (AMS) rozbaluje služby zabezpečení produktu IBM WebSphere 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

“IBM WebSphere MQ Advanced Message Security” na stránce 263
IBM WebSphere MQ Advanced Message Security (AMS) je samostatně licencovaná komponenta produktu IBM WebSphere MQ Advanced Message Security , která poskytuje vysokou úroveň ochrany citlivých dat procházejících přes síť IBM WebSphere MQ Advanced Message Security , 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 WebSphere MQ .

Produkt IBM WebSphere 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 WebSphere MQ nabízí celou řadu služeb zabezpečení na úrovni odkazů, včetně podpory zabezpečení SSL (Secure Sockets Layer) a TLS (Transport Layer Security).

Při implementaci produktu WebSphereje třeba vzít v úvahu určité aspekty zabezpečení. Pokud na systémech UNIX, Linux a Windows ignorujete tyto aspekty a nedělat nic, nemůžete použít produkt WebSphere MQ.

Bezpečnostní pokyny jsou popsány níže.

Oprávnění pro správu produktu WebSphere MQ

Administrátoři produktu WebSphere MQ potřebují oprávnění k:

- Zadejte příkazy pro správu produktu WebSphere MQ
- Použití Průzkumníka IBM WebSphere MQ

Další informace naleznete v následujících tématech:

- “Oprávnění k administraci produktu IBM WebSphere MQ v systémech UNIX, Linux, and Windows” na stránce 192

Oprávnění pro práci s objekty WebSphere MQ

Aplikace mohou přistupovat k následujícím objektům produktu WebSphere 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 produktu WebSphere MQ a také k přístupu k kanálům a objektům ověřovacích informací. Tyto objekty mohou být chráněny produktem WebSphere MQ , takže ID uživatelů přidružená k aplikacím potřebují oprávnění pro přístup k těmto objektům.

Další informace viz "Autorizace pro aplikace, které mají být použity IBM WebSphere MQ" na stránce 49.

Zabezpečení kanálu

ID uživatelů přidružená k agentům kanálu zpráv (MCA) potřebují oprávnění pro přístup k různým prostředkům produktu WebSphere 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 67.

Další pokyny

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

- "Zabezpečení klastrů správců front" na stránce 76
- "Zabezpečení pro publikování/odběr produktu IBM WebSphere MQ" na stránce 77
- "Zabezpečení pro IBM WebSphere MQ internet pass-thru" na stránce 78

Plánování identifikace a ověření

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

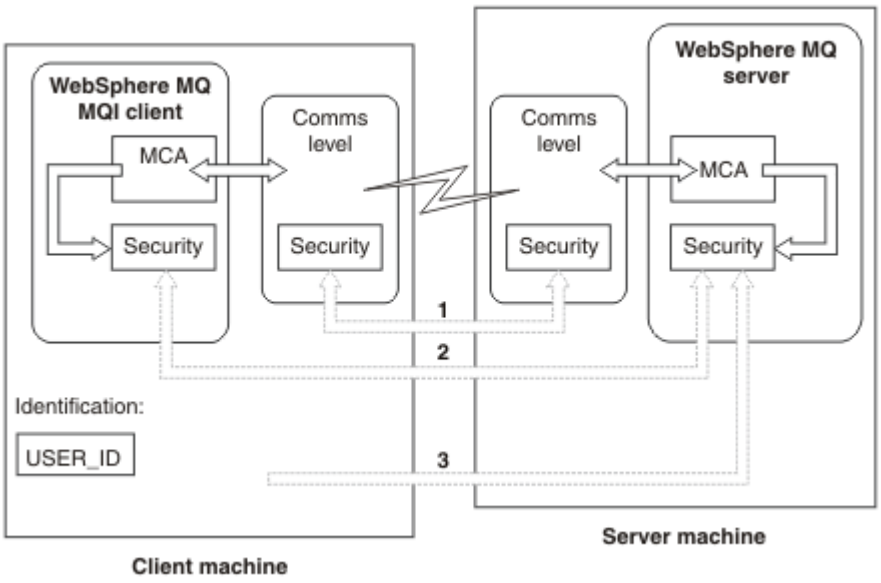
Musíte se rozhodnout, jak budete identifikovat uživatele vašich aplikací produktu IBM WebSphere MQ s ohledem na to, že různé operační systémy podporují ID uživatelů různých délek. Záznamy ověření kanálu můžete použít k mapování z jednoho ID uživatele na jiný, nebo k uvedení ID uživatele na základě atributu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

- "Mapování vzdáleného správce front na ID uživatele MCAUSER" na stránce 180
- "Mapování uživatelem deklarovaného ID uživatele na ID uživatele MCAUSER" na stránce 181
- "Mapování rozlišovacího jména SSL nebo TLS na ID uživatele MCAUSER" na stránce 181
- "Mapování adresy IP na ID uživatele MCAUSER" na stránce 183

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. Na diagramu je zobrazen klient IBM WebSphere MQ MQI, 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 7. Zabezpečení v připojení klient/server

1. Úroveň komunikace

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

2. Záznamy ověření kanálu

   Viz šipky 2 & 3. Ověřování lze řídit pomocí adres IP nebo rozlišujících názvů SSL/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 39.

3. 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.

4. 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 WebSphere 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.

   Klienti Windows také odesílají další informace pomáhající při identifikaci.

   - ID uživatele, které je předáno na server, je momentálně přihlášené ID uživatele na klientovi.
   - ID zabezpečení momentálně přihlášeného uživatele.

   Chcete-li pomoci při identifikaci klienta IBM WebSphere MQ pro produkt HP Integrity NonStop Server, klient předá alias OOSS Safeard alias, pod kterým je spuštěna klientská aplikace. Toto ID je obvykle ve tvaru <PRIMARYGROUP>.<ALIAS>. V případě potřeby můžete toto ID uživatele mapovat na alternativní ID uživatele ve správci front, a to buď pomocí záznamů ověření kanálu, nebo pomocí uživatelské procedury zabezpečení. Další informace o uživatelských procedurách pro zprávy naleznete v tématu “Mapování identit ve výstupních procedurách zprávy” na stránce 145. Další informace o definování záznamů ověření kanálu viz “Mapování uživatelem deklarovaného ID uživatele na ID uživatele MCAUSER” na stránce 181.

   Hodnoty ID uživatele a, je-li k dispozici, ID zabezpečení, mohou být použity uživatelskou procedurou zabezpečení serveru k vytvoření identity klienta IBM WebSphere MQ MQI.

ID uživatelů

Je-li klient IBM WebSphere MQ MQI na systému Windows a server IBM WebSphere MQ se také nachází v systému Windows a má přístup k doméně, na které je definováno ID uživatele klienta, produkt IBM WebSphere MQ podporuje ID uživatelů o maximální délce 20 znaků. Na platformách a konfiguracích systému UNIX and Linux je maximální délka 12 znaků.

Server WebSphere MQ for Windows nepodporuje připojení klienta Windows , pokud klient běží pod ID uživatele, který 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`.

Povšimněte si, že `UNKNOWN` je vyhrazené ID uživatele a ID uživatele produktu `NOBODY` má také speciální význam pro produkt WebSphere MQ. Vytvoření ID uživatelů v operačním systému s názvem `UNKNOWN` nebo `NOBODY` by mohlo mít nechtěné výsledky.

Ačkoli se ID uživatele používají k ověření, skupiny se používají pro autorizaci, kromě pro systém Windows.

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.

Plánování autorizace

Naplánujte uživatele, kteří budou mít administrativní oprávnění, a naplánujte, jakým způsobem mají uživatelé aplikací správně používat objekty produktu IBM WebSphere MQ , včetně těch, které se připojují z klienta IBM WebSphere MQ MQI.

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

- Oprávnění k provádění administrativních operací
- Autorizace pro aplikace pro použití produktu IBM WebSphere 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 pro administraci produktu IBM WebSphere MQ

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

Administrátoři produktu IBM WebSphere MQ potřebují oprávnění k:

- Vydat příkazy pro administraci produktu IBM WebSphere MQ
- PoužijteIBM WebSphere MQ Explorer

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

Oprávnění ke správě produktu IBM WebSphere MQ v systémech UNIX a Windows

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

Chcete-li být administrátorem produktu IBM WebSphere MQ v systémech UNIX a Windows , musí být uživatel členem skupiny *mqm*. Tato skupina se vytvoří automaticky při instalaci produktu WebSphere MQ. Chcete-li uživatelům povolit, aby mohli vydávat příkazy pro řízení, musíte je přidat do skupiny mqm. To zahrnuje uživatele root na systémech UNIX .

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

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

Všichni členové skupiny mqm mají přístup ke všem prostředkům produktu WebSphere MQ v systému, včetně možnosti administrovat 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 WebSphere MQ .

Administrátoři mohou použít řídicí příkaz **runmqsc** k vydání příkazu WebSphere 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 WebSphere MQ Explorer vydává příkazy PCF pro provádění administrativních úloh. Administrátoři nevyžadují žádné další oprávnění k administraci správce front v lokálním systému pomocí programu Průzkumník produktu WebSphere MQ . Je-li produkt WebSphere MQ Explorer použit ke správě správce front v jiném systému, administrátoři musí mít vyžadované oprávnění pro příkazy PCF, které mají být zpracovány vzdáleným správcem 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 WebSphere MQ” na stránce 49.
- Pro příkazy, které pracují s kanály, inicializátory kanálu, listenery a klastry, naleznete informace v tématu Zabezpečení kanálů.

Další informace o oprávnění, které potřebujete ke správě produktu WebSphere MQ na systémech UNIX a Windows , najdete v souvisejících informacích.

Autorizace pro aplikace, které mají být použity IBM WebSphere MQ

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

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

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

Aplikace mohou také používat příkazy PCF ke správě objektů IBM WebSphere 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.

Aplikace, které používají třídy IBM WebSphere MQ pro jazyk Java, třídy IBM WebSphere MQ pro platformu JMS, třídy IBM WebSphere MQ pro prostředí .NET nebo Message Service Clients for C/C++ and .NET , používají rozhraní MQI nepřímo.

MCAs také vydává volání MQI a uživatelská jména přidružená k objektu MCAs pro přístup k těmto objektům produktu WebSphere MQ . Další informace o těchto ID uživatelů a oprávněních, která vyžadují, najdete v tématu “Ověřování kanálu” na stránce 67.

Při provádění kontrol oprávnění

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

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 WebSphere MQ. Produkt IBM WebSphere MQ předpokládá, že uživatelé jsou přihlášeni k základnímu operačnímu systému a že jsou ověřeni pomocí tohoto systému.

Když aplikace otevře objekt IBM WebSphere 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 vzdáleným správcem front. V systému UNIX, Linux, and Windowsje 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 příkaz PCF, který pracuje na objektu WebSphere MQ , je 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 51.

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.

Oprávnění pro práci s objekty IBM WebSphere MQ na systémech UNIX, Linux a Windows

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

1. Ověřování.

   Kontrola ověření provedená pomocí OAM dodávaná s produktem IBM WebSphere 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, provede se kontrola nad funkcí OAM ve své funkci MQZID_AUTHENTICATE_USER. Jedná se o kontrolu: ID uživatele ve struktuře MQCSP je

porovnáno s ID uživatele v *IdentityContext* (MQZIC), aby bylo možné určit, zda se shodují. Pokud se neshodují, kontrola selže.

Tato základní kontrola není určena k úplnému ověření uživatele. Například, kontrola autenticity uživatele se neprovádí kontrolou hesla dodaného ve struktuře MQCSP. Pokud navíc aplikace vynechá strukturu MQCSP, nebude provedena žádná kontrola.

Jsou-li ve správci front vyžadovány podrobnější ověřovací služby prostřednictvím komponenty autorizační služby, produkt OAM poskytnutý s produktem IBM WebSphere MQ tuto hodnotu nenabízí. Musíte napsat novou komponentu autorizační služby, nebo ji získat od dodavatele.

2. 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 UNIX, Linux a Windows poskytuje *autorizační služba* řízení přístupu, když aplikace vydá volání MQI pro přístup k objektu IBM WebSphere 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.

V systému Windowsdává produkt OAM členům skupiny administrátorů oprávnění pro přístup ke všem objektům IBM WebSphere MQ i v případě, že je povolen přístup UAC.

Kromě toho má účet SYSTEM v systémech Windows úplný přístup k prostředkům produktu IBM WebSphere MQ .

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

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 WebSphere MQ .

Komponenta autorizační služba poskytovaná s produktem IBM WebSphere 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 IBM WebSphere MQ , ke kterému má řídicí přístup. V systémech UNIX and Linux se mohou v seznamu přístupových práv zobrazit pouze ID skupin. To znamená, že všichni členové skupiny mají stejné oprávnění. V systémech Windows se ID uživatelů a ID skupin mohou zobrazit v seznamu přístupových práv. 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 produkt Linux tento limit zvýšil, ale produkt IBM WebSphere MQ pokračuje ve sledování omezení 12 znaků na všech platformách UNIX . Použijete-li ID uživatele delší než 12 znaků, produkt IBM WebSphere MQ ji nahradí hodnotou "UNKNOWN". 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 WebSphere 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.

Na systémech UNIX, Linux a Windows příkaz řízení **setmqaut** uděluje a ruší 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.

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

Použití příkazu PCF pro přístup k příkazům OAM
V systémech UNIX, Linux a Windows můžete použít příkazy PCF pro přístup k příkazům administrace OAM.

Příkazy PCF a jejich ekvivalentní příkazy OAM jsou následující:

Tabulka 6. 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 .

Zabezpečení pro vzdálený systém zpráv

Tento oddíl pojednává o aspektech zabezpečení vzdáleného systému zpráv.

Musíte poskytnout uživatelům oprávnění k používání zařízení produktu IBM WebSphere 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: vzdálené IP adresy, jména vzdáleného uživatele, jména vzdáleného uživatele, SSL nebo jména vzdáleného správce front, implementujte záznamy ověření kanálu, nebo nastavte hodnotu MCAUSER na základě následujících údajů: vzdálené IP adresy, ID vzdáleného uživatele, SSL nebo TSL (Subject Distinguished Name) nebo jméno vzdáleného
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.

Zabezpečení objektů v systémech UNIX and Linux

Administrační uživatelé musí být součástí skupiny mqm na vašem systému (včetně uživatele root), pokud toto ID bude používat příkazy administrace produktu IBM WebSphere MQ .

Vždy byste měli spouštět příkaz amqcrsta jako ID uživatele "mqm".

ID uživatelů na systémech UNIX 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.

Zabezpečení objektů v systémech Windows

Administrační uživatelé musí být součástí skupiny mqm a skupiny administrátorů v systémech Windows , pokud toto ID bude používat příkazy administrace produktu IBM WebSphere MQ .

ID uživatelů na systémech Windows

V systémech Okna *pokud není nainstalována žádná uživatelská procedura pro zprávy*správce front převádí všechna velká nebo smíšená písmena uživatelů na malá a velká písmena 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.

ID uživatelů v rámci systémů

Platformy jiných než Windows , UNIX and Linux systémy používají velká písmena pro ID uživatelů ve zprávách.

Chcete-li umožnit systému Windows, aby systémy UNIX and Linux používaly malá ID uživatelů ve zprávách, budou na těchto platformách provedena následující konverze z agenta MCA (Message Channel Agent):

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.

Pokud poskytnete ukončení zpráv v systémech UNIX, Linux a Windows z jakékoli jiné příčiny, neprovedou se automatické převody.

Použití vlastní autorizační služby

Produkt IBM WebSphere MQ poskytuje instalovatelnou autorizační službu. Můžete zvolit instalaci alternativní služby.

Komponenta autorizační služba dodaná s produktem IBM WebSphere 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 WebSphere 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 7. 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 57 .
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 použité ID 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 57 .

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 klienty IBM WebSphere MQ MQI je 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.

Ujistěte se, že pole MCAUSER je omezeno na 12 znaků na platformách Windows, protože všechny přebytečné znaky budou zkráceny, což může vést k selhání autorizace.

Klient produktu IBM WebSphere 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:

- 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 WebSphere 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 WebSphere 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.

V případě serverů v systémech UNIX, Linux a Windows se obsah pole `MCAUserIdentifier` , které je přijatý od klienta, změní na malá písmena.

U serverů v systému IBM ise obsah pole `LongMCAUserIdentifier` přijatého od klienta změní na velká písmena.

U serverů v systémech UNIX and Linux je obsah pole `LongMCAUserIdentifier` obdržený od klienta změněn na malá písmena.

ID uživatele, které je předáno při použití aplikace vazby MQ JMS , je standardně 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 zvolit použití SSL nebo TLS, v tom případě si 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 58
Toto téma obsahuje informace o různých aspektech zabezpečení na úrovni odkazů a zabezpečení na úrovni aplikací a porovnává dvě úrovně zabezpečení.

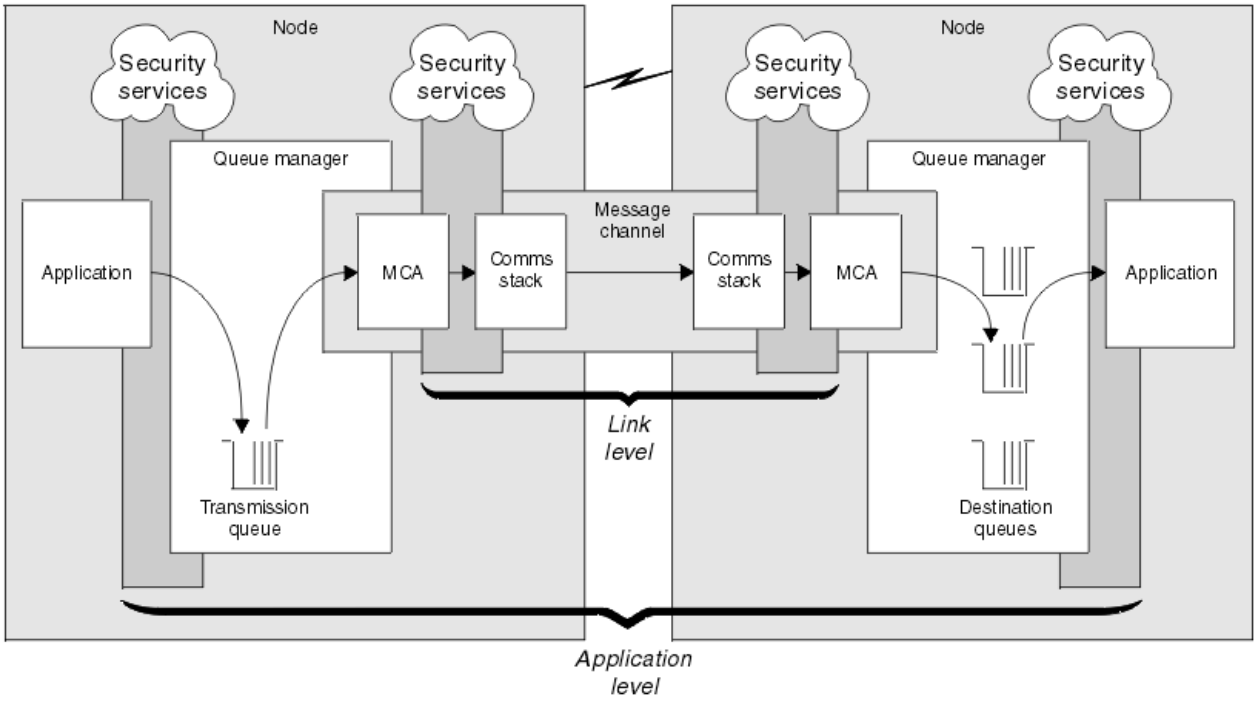
“Ukončovací programy kanálu” na stránce 63
Ukončovací programy kanálu jsou programy, které jsou volány v definovaných místech v posloupnosti zpracování agenta MCA. Uživatelé a dodavatelé mohou napsat své vlastní uživatelské programy kanálu. Některé jsou dodávány společností IBM.

“Ochrana kanálů pomocí SSL” na stránce 69
Podpora SSL v produktu IBM WebSphere 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 8 na stránce 59.



Obrázek 8. 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.

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. Jedná se o hlavní rozdíl mezi zabezpečením na úrovni odkazů a zabezpečením na úrovni aplikace a je zobrazen v tématu Obrázek 8 na stránce 59.

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 WebSphere 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 nelze chránit data v rámci toků protokolů kanálu WebSphere MQ , které nejsou daty zprávy. 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 tématu Obrázek 8 na stránce 59.

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 WebSphere MQ

Primárním prostředkem pro zajištění důvěrnosti a integrity dat v produktu IBM WebSphere MQ je použití zabezpečení SSL nebo TLS. Další informace o použití SSL a TLS v produktu IBM WebSphere MQviz "Podpora produktu IBM WebSphere MQ pro zabezpečení SSL a TLS" na stránce 23. Pro ověření poskytuje produkt IBM WebSphere 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 39.

Poskytnutí zabezpečení na úrovni vlastního odkazu
Tato kolekce témat popisuje, jak můžete poskytovat 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 63. Stejné téma také popisuje ukončovací program kanálu, který je dodáván s produktem IBM WebSphere MQ for Windows (uživatelský ukončovací program 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 WebSphere MQ, nebo kombinací libovolné z těchto pracovních procesů. Zabezpečení na úrovni aplikace je ilustrováno v tématu Obrázek 8 na stránce 59.

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

IBM WebSphere MQ Advanced Message Security (AMS) je samostatně licencovaná komponenta produktu IBM WebSphere MQ , která poskytuje vysokou úroveň ochrany citlivých dat procházejících přes síť IBM WebSphere 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 WebSphere MQ. Tato řešení však vyžadují specializované dovednosti a mohou být složité a nákladné udržovat. Produkt IBM WebSphere MQ Advanced Message Security pomáhá řešit tyto problémy při přesouvání informací v podniku prakticky ve všech typech komerčních informačních systémů.

Produkt IBM WebSphere MQ Advanced Message Security rozšiřuje funkce zabezpečení produktu IBM WebSphere 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 WebSphere MQ servery, tak klienty.
- Poskytuje integraci s produktem IBM WebSphere MQ Managed File Transfer a poskytuje řešení zabezpečeného systému zpráv typu end to-end.

Další informace viz "IBM WebSphere MQ Advanced Message Security" na stránce 263.

Zajištění vlastního zabezpečení na úrovni aplikace
Tato kolekce témat popisuje, jak můžete poskytovat své vlastní služby zabezpečení na úrovni aplikace.

Pro usnadnění implementace zabezpečení na úrovni aplikací poskytuje produkt IBM WebSphere MQ dva uživatelské procedury, uživatelské procedury rozhraní API a ukončení přejezdu rozhraní API.

Tyto uživatelské procedury mohou poskytovat identifikaci a ověření, řízení přístupu, utajení, integritu dat a služby neodmítání a další funkce, které se nevztahují k zabezpečení.

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 WebSphere 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 WebSphere 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.

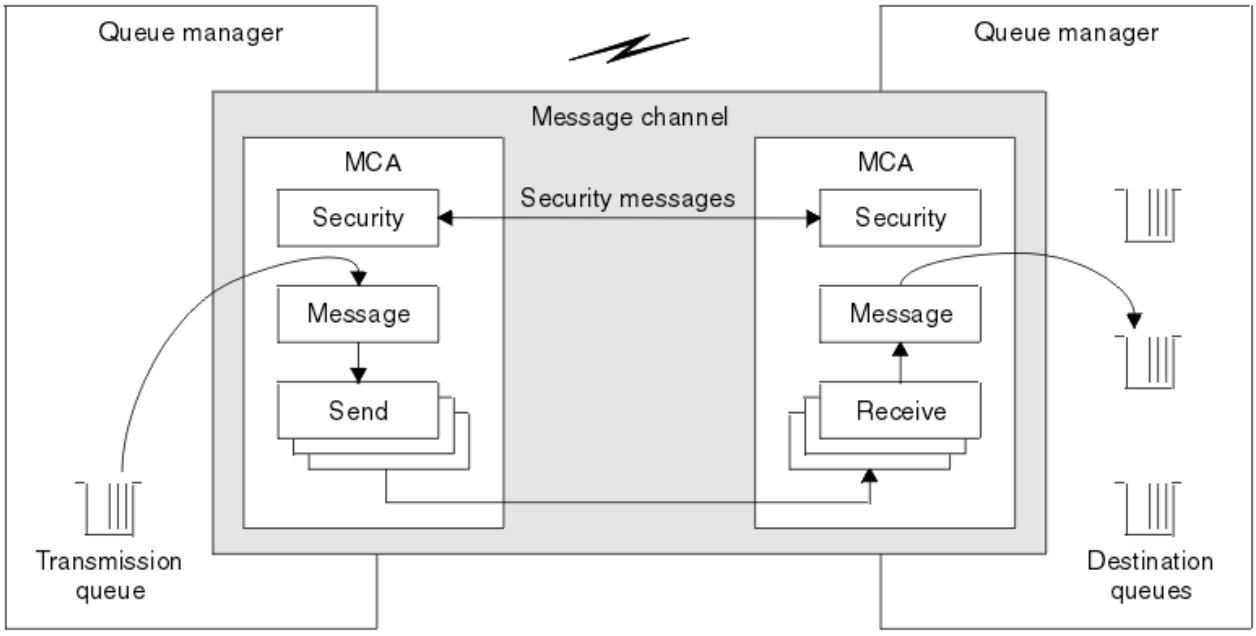
Ukončovací programy kanálu

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 společností 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 ilustrovány v části Obrázek 9 na stránce 64 a jsou popsány v následujících tématech.



Obrázek 9. 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 naleznete v tématu “Zabezpečení na úrovni odkazu pomocí uživatelské procedury zabezpečení” na stránce 61.

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. This is because the purpose of an MQI channel is to enable the input and output parameters of MQI calls to flow between the IBM WebSphere MQ MQI client application and the queue manager.

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 61.

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 WebSphere 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 WebSphere 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 odesílání a příjmu naleznete v tématu “Zabezpečení na úrovni odkazu pomocí uživatelských procedur pro odesílání a příjem” na stránce 61.

Plánování integrity dat

Naplánujte, jak zachovat integritu vašich dat.

Integritu dat můžete implementovat na úrovni aplikace nebo na úrovni odkazů.

Na úrovni aplikace se můžete rozhodnout používat produkt IBM WebSphere MQ Advanced Message Security k digitálnímu podpisu zpráv za účelem ochrany proti neautorizované úpravě. Ukončovací programy rozhraní API můžete použít také v případě, že standardní vybavení nesplňuje vaše požadavky.

Na úrovni linky se můžete rozhodnout použít SSL nebo TLS, v takovém případě musíte naplánovat použití digitálních certifikátů. Ukončovací programy kanálu můžete také použít, pokud standardní vybavení nevyhovují vašim požadavkům.

Související pojmy

“Ochrana kanálů pomocí SSL” na stránce 69
Podpora SSL v produktu IBM WebSphere MQ používá objekt ověřovacích informací správce front a různé příkazy MQSC. Musíte také zvážit použití digitálních certifikátů.

“Integrita dat v produktu IBM WebSphere MQ” na stránce 22
Službu integrity dat můžete použít ke zjištění, zda byla zpráva upravena.

“Plánování pro databázi Advanced Message Security” na stránce 62
IBM WebSphere MQ Advanced Message Security (AMS) je samostatně licencovaná komponenta produktu IBM WebSphere MQ , která poskytuje vysokou úroveň ochrany citlivých dat procházejících přes síť IBM WebSphere 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 WebSphere 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 WebSphere MQ pomocí rozhraní produktu IBM WebSphere MQ
Konfigurujte produkt IBM WebSphere MQ , chcete-li vydat události přípravy nástrojů, zejména události příkazů a události konfigurace.

Změny provedené v produktu IBM WebSphere MQ mimo jeho ovládací prvek
Některé změny mohou ovlivnit chování, jak se produkt IBM WebSphere MQ chová, ale nelze jej přímo monitorovat produktem IBM WebSphere 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 WebSphere 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 WebSphere MQ nakonfigurován, aby vydal události přípravy nástrojů.

Aktivita aplikace v produktu IBM WebSphere MQ
Chcete-li monitorovat akce aplikací, například otevírání front a vkládání zpráv a získávání zpráv, nakonfigurujte produkt IBM WebSphere MQ , aby vydal příslušné 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 WebSphere 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

S produktem IBM WebSphere MQ Explorerse dodává sada testů. 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

Při odeslání nebo přijetí zprávy prostřednictvím kanálu potřebujete uživatelské jméno, které má přístup k různým prostředkům produktu IBM WebSphere MQ .

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 WebSphere MQmohou být kanály chráněny podporou zabezpečení SSL nebo TLS.

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 .
- Pomocí ID uživatele asociovaného 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 WebSphere 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 bude mít úplná administrativní práva a nevyžaduje žádná speciální oprávnění.

    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.
  – Použijete-li ID uživatele, které nemá oprávnění k administraci produktu WebSphere , musíte pro kanál k práci udělit oprávnění dsp a ctrlx pro daný kanál. 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. Zadejte například následující příkazy:

```
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 39
Chcete-li zlepšit kontrolu nad udílením přístupu k připojujícím se systémům na úrovni kanálu, můžete použít záznamy ověření kanálu.

Vlastnosti záznamu ověření kanálu

Zabezpečení definic inicializátoru kanálu
Inicializátory inicializátorů kanálu mohou manipulovat pouze členové skupiny mqm.

Inicializátory kanálu produktu IBM WebSphere MQ nejsou objekty produktu IBM WebSphere MQ ; přístup k nim není řízen produktem OAM. Produkt IBM WebSphere 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 uvedené 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 odeslat zprávu přímo do přenosové fronty, vyžaduje to zvláštní oprávnění; viz Tabulka 10 na stránce 88.

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 63 .

Ochrana kanálů pomocí SSL
Podpora SSL v produktu IBM WebSphere MQ používá objekt ověřovacích informací správce front a různé příkazy MQSC. Musíte také zvážit použití digitálních certifikátů.

Příkazy a atributy pro podporu SSL

Protokol SSL (Secure Sockets Layer) poskytuje zabezpečení kanálu, s ochranou proti odposlouchávání, falšování a zosobnění. Podpora produktu IBM WebSphere MQ pro zabezpečení SSL umožňuje určit v definici kanálu to, že konkrétní kanál používá zabezpečení SSL. Můžete také uvést podrobnosti o typu zabezpečení, jaký chcete, jako například šifrovací algoritmus, který chcete použít.

Následující příkazy MQSC podporují zabezpečení SSL:

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 zabezpečení SSL:

SSLCRLNL
Atribut SSLCRLNL určuje seznam názvů objektů ověřovacích informací, které se používají k poskytování umístění odvolaných certifikátů, které umožňují lepší kontrolu certifikátu TLS/SSL.

SSLCRYP
V systémech Windows, UNIX and Linux , nastavuje atribut správce front 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 SSL ohlášena, pokud kanál používající zabezpečení SSL selže při navázání připojení SSL.

SSLFIPS
Určuje, zda mají být použity pouze algoritmy certifikované podle standardu FIPS, pokud je šifrování prováděno v produktu IBM WebSphere 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
Na systémech Windows,UNIX and Linux , přidružuje úložiště klíčů ke správci front. Databáze klíčů je zadržena v databázi klíčů *GSKit* . (Produkt IBM Global Security Kit (GSKit) umožňuje použít zabezpečení SSL na systémech Windows,UNIX and Linux .)

SSLRKEYC
Počet bajtů, které mají být odeslány a přijaty v rámci konverzace SSL, než je znovu vyjednán tajný klíč. Počet bajtů zahrnuje řídicí informace odeslané agentem MCA.

Následující parametry kanálu podporují zabezpečení SSL:

SSLCAUTH
Definuje, zda produkt IBM WebSphere MQ vyžaduje a ověřuje certifikát od klienta SSL.

SSLCIPH
Určuje sílu a funkci šifrování (CipherSpec), například NULL_MD5 nebo RC4_MD5_US. Shoda CipherSpec musí odpovídat oběma konci kanálu.

SSLPEER
Uvádí rozlišující název (jedinečný identifikátor) povolených partnerů.

Tento oddíl popisuje příkazy `setmqaut`, `dspmqaut`, `dmpmqaut`, `rcrmqobj`, `rcdmqimga` `dspmqfls` pro podporu objektu ověřovacích informací. Popisuje také příkaz iKeycmd pro správu certifikátů v systémech UNIX and Linux a nástroj runmqakm pro správu certifikátů na systémech UNIX, Linux a Windows . Viz následující sekce:

- setmqaut
- dspmqaut
- dmpmqaut
- rcrmqobj
- rcdmqimg
- dspmqfls
- Správa klíčů a certifikátů

Přehled zabezpečení kanálu pomocí SSL viz

- “Podpora produktu IBM WebSphere MQ pro zabezpečení SSL a TLS” na stránce 23

Podrobnosti o příkazech MQSC přidružených k protokolu SSL viz

- ALTER AUTHINFO
- Příkaz DEFINE AUTHINFO
- ODSTRANIT AUTHINFO
- ZOBRAZIT AUTHINFO

Podrobnosti o příkazech PCF přidružených k SSL viz

- Změnit, kopírovat a vytvořit objekt ověřovacích informací
- Odstranit objekt ověřovacích informací
- Dotaz na objekt ověřovacích informací

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:

Na systémech Windows, UNIXa Linux můžete použít certifikáty podepsané sebou samým. Pokyny naleznete v příručce “Vytvoření osobního certifikátu s automatickým podpisem na systémech UNIX, Linux, and Windows” na stránce 119 .

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 váš digitální certifikát. Podobně platí, že pokud vaše zásada zabezpečení vaší organizace vyžaduje použití určité CipherSpec , je třeba získat vhodný digitální certifikát.

Další informace o vztahu mezi CipherSpecs a digitálními certifikáty viz “Digitální certifikáty a kompatibilita CipherSpec v produktu IBM WebSphere MQ” na stránce 34

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 WebSphere MQnaleznete v tématu “Zásady ověření platnosti certifikátu v produktu IBM WebSphere MQ” na stránce 33.

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 WebSphere 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 šifrování Triple DES 24 bajtů v systému z/OS, najdete v dokumentaci.

Další obecné informace o šifrování na úrovni relace najdete v tématu *Systems Network Architecture LU 6.2 Reference: Peer Protocols*, SC31-6808.

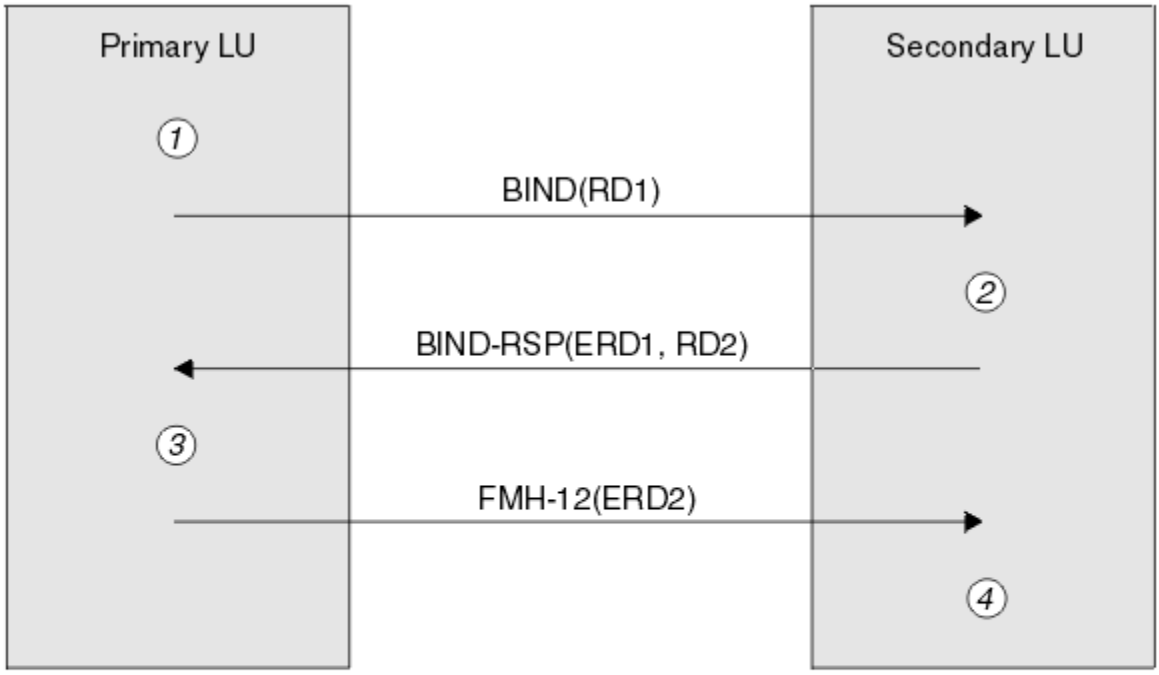
Ověření úrovně relace

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 10 na stránce 73 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 10. Toky pro ověření na úrovni relace

Protokol pro ověření úrovně relace je následující. Čísla v proceduře odpovídají číslům v produktu Obrázek 10 na stránce 73.

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*.

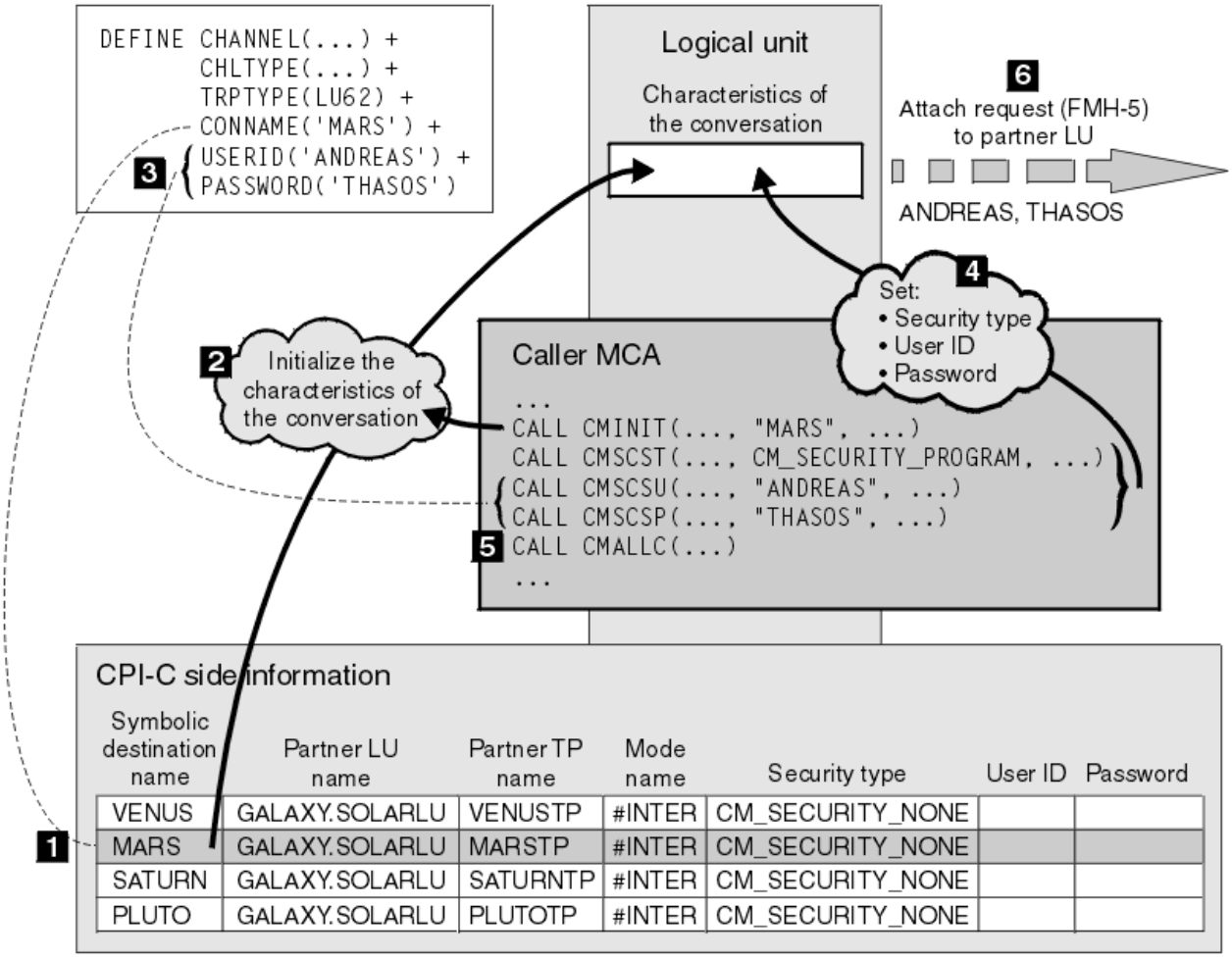
Následující témata popisují, jak produkt IBM WebSphere MQ poskytuje podporu pro ověření na úrovni konverzace.

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 MVS 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 TP Callable Services naleznete v příručce *z/OS MVS Programming: Writing Transaction Programs for APPC/MVS*, SA22-7621.

Podpora pro ověření na úrovni konverzace v produktu IBM WebSphere MQ v systémech UNIX a Windows
V tomto tématu získáte přehled o tom, jak funguje ověřování na úrovni konverzace, v systému UNIX, Linux, and Windows.

Podpora pro ověření na úrovni konverzace v produktu IBM WebSphere MQ pro produkt WebSphere MQ na systémech UNIX a WebSphere MQ for Windows je ilustrován v tématu Obrázek 11 na stránce 75. Čísla v diagramu odpovídají číslům v níže uvedeném popisu.



Obrázek 11. Podpora produktu WebSphere MQ pro ověření na úrovni konverzace

V systémech IBM i, systémech UNIX a Windows 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.

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 WebSphere MQ se rozhodne, kterému správci front má odeslat. Když mnoho aplikací odesílá zprávy do fronty klastru, produkt WebSphere MQ vyrovnává pracovní zátěž mezi všemi správci front, kteří mají instanci fronty. Pokud jeden ze systémů, který je hostitelem klonovaného správce front, selže, produkt WebSphere MQ bude 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.

Související úlohy

“Zabránění příjmu zpráv správcem front” na stránce 243
Můžete zabránit správci front klastru, aby přijímal zprávy, které nemá oprávnění přijímat, pomocí ukončovacích programů.

Zabezpečení pro publikování/odběr produktu IBM WebSphere MQ

Používáte-li produkt IBM WebSphere 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 WebSphere 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 WebSphere 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 WebSphere MQ .

Výběrové vysílání produktu IBM WebSphere 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 WebSphere MQ (například aplikace LLM, viz Multicast Interoperability with WebSphere MQ Low Latency Messaging), 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 WebSphere MQ je založeno na ID uživatelů. Další informace o tomto tématu viz “Řízení přístupu pro klienty” na stránce 56.

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 v produktu IBM WebSphere MQdočasně blokovat adresy IP, možná byste měli počkat na administrátora zabezpečení, aby aktualizoval pravidla brány firewall.

Chcete-li blokovat jednu nebo více adres IP, vytvořte záznam ověřování kanálu typu BLOCKADDR nebo ADDRESSMAP. Více informací naleznete v části “Blokování určitých adres IP” na stránce 178.

Zabezpečení pro IBM WebSphere MQ internet pass-thru

Internet pass-through může zjednodušit komunikaci přes firewall, ale to má bezpečnostní důsledky.

IBM WebSphere MQ -přímý průchod je základním rozšířením produktu IBM WebSphere MQ dodávaným v balíku SupportPac MS81.

WebSphere MQ internet pass-thru umožňuje dvěma správcům front výměnu zpráv nebo klientskou aplikaci WebSphere 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 WebSphere MQ do a ven z brány firewall jednodušší a lépe spravovatelný tunelováním toků uvnitř HTTP nebo se jedná o server proxy. Při použití SSL (Secure Sockets Layer) lze také použít k šifrování a dešifrování zpráv, které jsou odesílány přes Internet.

Pokud váš systém WebSphere MQ komunikuje s IPT, pokud nepoužíváte SSLProxyMode v IPT, ujistěte se, že CipherSpec používaná produktem WebSphere MQ odpovídá sadě CipherSuite použité IPT:

- Pokud IPT vystupuje jako server zabezpečení SSL nebo TLS a produkt WebSphere MQ se připojuje jako klient SSL nebo TLS, musí CipherSpec používaná produktem WebSphere MQ odpovídat sadě CipherSuite , která je povolena v příslušném svazku klíčů IPT.

- Pokud IPT vystupuje jako klient SSL nebo TLS a připojuje se k serveru WebSphere MQ SSL nebo TLS, musí IPT CipherSuite odpovídat sadě CipherSpec definované na přijímajícím kanálu produktu WebSphere MQ .

Pokud migrujete z IPT na integrovanou podporu SSL a TLS produktu WebSphere MQ , přeneste digitální certifikáty z IPT pomocí iKeyman.

Další informace naleznete v dokumentu WebSphere MQ Internet Pass-Thru (SupportPac MS81).

Nastavení zabezpečení

Tato kolekce témat obsahuje informace specifické pro různé operační systémy a také pro použití klientů.

Nastavení zabezpečení na systémech UNIX, Linux, and Windows

Aspekty zabezpečení specifické pro systémy UNIX, Linux, and Windows .

Správci front produktu IBM WebSphere 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 WebSphere MQ
Můžete definovat sadu uživatelů, kteří mohou vydávat příkazy pro administraci produktu IBM WebSphere MQ.

Kdo může používat objekty produktu IBM WebSphere 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 WebSphere 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 WebSphere MQsoukromý; nepoužívejte standardní příkazy operačního systému k udělení nebo zrušení autorizace k prostředkům MQI.

Připojení k produktu IBM WebSphere MQ pomocí Terminal Services

Právo uživatele **Create global objects** může způsobit problémy, pokud používáte Terminal Services.

Pokud se připojujete k systému Windows pomocí služeb Terminal Services a máte problémy s vytvářením nebo spouštěním správce front, může to být způsobeno tím, že uživatel má právo **Create global objects**, v posledních verzích systému Windows.

Uživatelské právo **Create global objects** 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 právo na uživatele **Create global objects** , které se na něj používá.

Administrátoři mají při výchozím nastavení nárok uživatele **Create global objects** , takže administrátor může vytvořit a spustit správce front při připojení pomocí služeb Terminal Services bez změny práv uživatele.

Pokud různé metody administrace produktu WebSphere MQ nefungují při použití terminálových služeb, pokuste se nastavit uživatele **Create global objects** správně:

1. Otevřete panel Administrativní nástroje:

   Windows 2003 a Windows XP
   Do tohoto panelu přistupte pomocí nabídky **Ovládací panely** > **Nástroje pro správu**.

   Windows Vista a Windows Server 2008
   Tento panel otevřete pomocí nabídky **Ovládací panely** > **Systém a údržba** > **Administrativní nástroje**.
2. Poklepejte na položku **Lokální zásada zabezpečení**.
3. Rozbalte `Local Policies`.
4. Klepněte na tlačítko `User Rights Assignment`.
5. Přidejte nového uživatele nebo skupinu do zásady **Create global objects** .

Vytvoření a správa skupin v systému Windows

Tyto pokyny vás vedou procesem administrace skupin na počítači pracovní stanice nebo na počítači s členskými servery.

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 vydáte příkaz MQSC REFRESH SECURITY (nebo ekvivalent PCF).

Použijte panel Správa počítače pro práci s uživateli a skupinami. Jakékoli změny provedené u aktuálně přihlášeného uživatele nemusí být účinné, dokud se uživatel znovu nepřihlásí.

Windows 2003 a Windows XP
Tento panel otevřete pomocí nabídky **Ovládací panely** > **Administrativní nástroje** > **Správa počítačů**.

Windows Vista a Windows Server 2008
Tento panel otevřete pomocí voleb **Ovládací panely** > **Systém a údržba** > **Administrativní nástroje** > **Správa počítačů**.

Windows 7.
Otevřete tento panel pomocí nabídky **Administrativní nástroje** > **Správa počítačů** .

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**.

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.

Zobrazení uživatelů 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.

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.

Vytvoření a správa skupin v systému HP-UX

V systému HP-UX, pokud nepoužíváte NIS nebo NIS +, použijte nástroj System Administration Manager (SAM) pro práci se skupinami.

Vytvoření skupiny v systému HP-UX
Přidání uživatele do skupiny pomocí produktu System Administration Manager

Postup

1. Ve správci správy systému (SAM) dvakrát klepněte na účty pro uživatele a skupiny.
2. Poklepejte na Skupiny.
3. Chcete-li zobrazit panel Přidat novou skupinu, vyberte volbu Přidat z rozbalovací nabídky Akce.
4. Zadejte název skupiny a vyberte uživatele, které chcete přidat do skupiny.
5. Klepnutím na tlačítko Použít vytvoříte skupinu.

Výsledky
Nyní jste vytvořili skupinu.

Přidání uživatele do skupiny v systému HP-UX
Přidejte uživatele do skupiny pomocí produktu System Administration Manager.

Postup

1. Ve správci správy systému (SAM) dvakrát klepněte na účty pro uživatele a skupiny.
2. Poklepejte na Skupiny.
3. Zvýrazněte název skupiny a z rozbalovací nabídky Akce vyberte volbu Upravit, aby se zobrazil panel Upravit existující skupinu.
4. Vyberte uživatele, kterého chcete přidat do skupiny, a klepněte na tlačítko Přidat.
5. Chcete-li přidat další uživatele do skupiny, zopakujte krok 4 pro každého uživatele.
6. Jakmile dokončíte přidávání jmen do seznamu, klepněte na OK.

Výsledky
Nyní jste přidali uživatele do skupiny.

Zobrazení uživatelů ve skupině v systému HP-UX
Zobrazení toho, kdo je ve skupině, pomocí správce administrace systému

Postup

1. Ve správci správy systému (SAM) dvakrát klepněte na účty pro uživatele a skupiny.
2. Poklepejte na Skupiny.
3. Zvýrazněte název skupiny a vyberte volbu Upravit ze stahovacího seznamu Akce, abyste zobrazili panel Upravit existující skupinu a zobrazili seznam uživatelů ve skupině.

Výsledky
Zobrazí se členové skupiny.

Odebrání uživatele ze skupiny v systému HP-UX
Odebrání uživatele ze skupiny pomocí nástroje System Administration Manager.

Postup

1. Ve správci správy systému (SAM) dvakrát klepněte na účty pro uživatele a skupiny.
2. Poklepejte na Skupiny.
3. Zvýrazněte název skupiny a z rozbalovací nabídky Akce vyberte volbu Upravit, aby se zobrazil panel Upravit existující skupinu.
4. Vyberte uživatele, kterého chcete odebrat ze skupiny, a klepněte na tlačítko Odebrat.
5. Chcete-li odebrat další uživatele ze skupiny, zopakujte krok 4 pro každého uživatele.
6. Po dokončení odebírání názvů ze seznamu klepněte na tlačítko OK.

Výsledky
Nyní jste odebrali uživatele ze skupiny

Vytvoření a správa skupin v systému AIX

V systému AIX, pokud nepoužíváte NIS nebo NIS +, použijte SMITTY pro práci se skupinami.

Vytvoření skupiny
Vytvořte skupinu pomocí SMITTY.

Postup

1. Ze souboru SMITTY vyberte volbu Zabezpečení a Uživatelé a stiskněte klávesu Enter.
2. Vyberte skupiny a stiskněte klávesu Enter.
3. Vyberte volbu Přidat skupinu a stiskněte klávesu Enter.
4. Zadejte název skupiny a názvy všech uživatelů, které chcete přidat do skupiny, a oddělte je čárkami.
5. Chcete-li vytvořit skupinu, stiskněte klávesu Enter.

Výsledky
Nyní jste vytvořili skupinu.

Přidání uživatele do skupiny
Přidejte uživatele do skupiny pomocí příkazu SMITTY.

Postup

1. Ze souboru SMITTY vyberte volbu Zabezpečení a Uživatelé a stiskněte klávesu Enter.
2. Vyberte skupiny a stiskněte klávesu Enter.
3. Vyberte Změnit/Zobrazit vlastnosti skupin a stiskněte klávesu Enter.
4. Zadejte název skupiny, abyste zobrazili seznam členů skupiny.
5. Přidejte jména uživatelů, které chcete přidat do skupiny, a oddělte je čárkami.
6. Stisknutím klávesy Enter přidejte jména do skupiny.

Zobrazení uživatele ve skupině

Zobrazení uživatelů ve skupině používající SMITTY.

Postup

1. Ze souboru SMITTY vyberte volbu Zabezpečení a Uživatelé a stiskněte klávesu Enter.
2. Vyberte skupiny a stiskněte klávesu Enter.
3. Vyberte Změnit/Zobrazit vlastnosti skupin a stiskněte klávesu Enter.
4. Zadejte název skupiny, abyste zobrazili seznam členů skupiny.

Výsledky

Zobrazí se členové skupiny.

Odebrání uživatele ze skupiny

Odstranění uživatele ze skupiny pomocí SMITTY.

Postup

1. Ze souboru SMITTY vyberte volbu Zabezpečení a Uživatelé a stiskněte klávesu Enter.
2. Vyberte skupiny a stiskněte klávesu Enter.
3. Vyberte Změnit/Zobrazit vlastnosti skupin a stiskněte klávesu Enter.
4. Zadejte název skupiny, abyste zobrazili seznam členů skupiny.
5. Odstraňte jména uživatelů, které chcete odebrat ze skupiny.
6. Stisknutím klávesy Enter odeberete jména ze skupiny.

Výsledky

Nyní jste odebrali uživatele ze skupiny.

Vytvoření a správa skupin v systému Solaris

V systému Solaris za předpokladu, že nepoužíváte NIS nebo NIS +, použijte soubor `/etc/group` pro práci se skupinami.

Vytvoření skupiny v systému Solaris

Vytvoření skupiny pomocí příkazu **groupadd** .

Postup

Zadejte následující příkaz: `groupadd` *`group-name`*

kde *název-skupiny* je název skupiny.

Výsledky

Soubor `/etc/group` obsahuje informace o skupině.

Přidání uživatele do skupiny v systému Solaris
Přidejte uživatele do skupiny pomocí příkazu **usermod** .

Postup

Chcete-li přidat člena do doplňkové skupiny, proveďte příkaz `usermod` a zobrazte seznam doplňkových skupin, kterých se uživatel aktuálně nachází, a doplňkových skupin, kterých se má uživatel stát členem. Je-li například uživatel členem skupiny `groupa`a stane se členem `groupb` , použijte následující příkaz: `usermod -G groupa,groupb` *`user-name`* , kde *jméno-uživatele* je jméno uživatele.

Zobrazení uživatelů ve skupině v systému Solaris
Chcete-li zjistit uživatele, který je členem skupiny, podívejte se na položku této skupiny v souboru `/etc/group` .

Odebrání uživatele ze skupiny v systému Solaris
Odstranění uživatele ze skupiny pomocí příkazu **usermod** .

Postup

Chcete-li odebrat člena z doplňkové skupiny, proveďte příkaz **usermod** se seznamem doplňkových skupin, na které má uživatel zůstat členem.
Je-li například primární skupina uživatele `users` a uživatel je také členem skupin `mqm`, `groupa` a `groupb`, aby uživatel odebral uživatele ze skupiny `mqm` , použije se následující příkaz: `usermod -G groupa,groupb` *`user-name`*, kde *`user-name`* je jméno uživatele.

Vytvoření a správa skupin v systému Linux

V systému Linuxza předpokladu, že nepoužíváte NIS nebo NIS +, použijte soubor `/etc/group` pro práci se skupinami.

Vytvoření skupiny v systému Linux
Vytvořte skupinu pomocí příkazu **groupadd** .

Postup

Chcete-li vytvořit novou skupinu, zadejte následující příkaz: `groupadd -g` *`group-ID group-name`*
, kde *ID-skupiny* je číselný identifikátor skupiny, a *název-skupiny* je název skupiny.

Výsledky
Soubor `/etc/group` obsahuje informace o skupině.

Přidání uživatele do skupiny v systému Linux
Přidejte uživatele do skupiny pomocí příkazu **usermod** .

Postup

Chcete-li přidat člena do doplňkové skupiny, proveďte příkaz `usermod` a zobrazte seznam doplňkových skupin, kterých se uživatel aktuálně nachází, a doplňkových skupin, kterých se má uživatel stát členem. Je-li například uživatel členem skupiny `groupa`a stane se členem `groupb` , použije se následující příkaz: `usermod -G groupa,groupb` *`user-name`*
, kde *`user-name`* je jméno uživatele.

Zobrazení uživatele ve skupině v systému Linux
Obrazovka, která je ve skupině, pomocí příkazu **getent** .

Postup

Chcete-li zobrazit uživatele, který je členem skupiny, zadejte následující příkaz: `getent group` *`group-name`*

, kde *název-skupiny* je název skupiny.

Odebrání uživatele ze skupiny

Odstranění uživatele ze skupiny pomocí příkazu **usermod** .

Postup

Chcete-li odebrat člena z doplňkové skupiny, proveďte příkaz **usermod** se seznamem doplňkových skupin, na které má uživatel zůstat členem.
Je-li například primární skupina uživatele `users` a uživatel je také členem skupin `mqm`, `groupa` a `groupb`, aby uživatel odebral uživatele ze skupiny `mqm` , použije se následující příkaz: `usermod -G groupa,groupb` *`user-name`*

, kde *jméno-uživatele* je jméno uživatele.

Jak autorizací fungují

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 tyto konstanty v seznamu oprávnění příkazu `setmqaut` pro danou entitu v seznamu oprávnění příkazu MQZAO_. Například MQZA_BROWSE odpovídá klíčovému slovu `+browse`, hodnota MQZAO_SET_ALL_CONTEXT odpovídá klíčovému slovu `+setall`atd. Tyto konstanty jsou definovány v souboru záhlaví cmqzc.hdodaném spolu s produktem.

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 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 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 8 na stránce 87, Tabulka 9 na stránce 87, Tabulka 10 na stránce 88a Tabulka 11 na stránce 88 shrnují autorizace potřebné 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 8. Autorizace zabezpečení potřebná pro volání MQCONN

Je vyžadována autorizace pro:	**Objekt fronty (“1” na stránce 88)**	**Objekt procesu**	**Objekt správce front**
MQCONN	Nelze použít	Nelze použít	MQZAO_PŘIPOJENÍ

Tabulka 9. Autorizace zabezpečení potřebná pro volání MQOPEN

Je vyžadována autorizace pro:	**Objekt fronty (“1” na stránce 88)**	**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 89)**	MQZAO_VSTUP	Nelze použít	Nelze použít
MQOO_OUTPUT (normální fronta) **(“3” na stránce 89)**	MQZAO_VÝSTUP	Nelze použít	Nelze použít
MQOO_PASS_ IDENTITY_CONTEXT **(“4” na stránce 89)**	MQZAO_PASS_ IDENTITY_CONTEXT	Nelze použít	Žádná kontrola
MQOO_PASS_ALL_ CONTEXT **(“4” na stránce 89, “5” na stránce 89)**	MQZAO_PASS _ALL_CONTEXT	Nelze použít	Žádná kontrola
MQOO_SET_ IDENTITY_CONTEXT **(“4” na stránce 89, “5” na stránce 89)**	MQZAO_SET_ IDENTITY_CONTEXT	Nelze použít	MQZA_SET_ IDENTITY_CONTEXT **(“6” na stránce 89)**
MQOO_SET_ ALL_CONTEXT **(“4” na stránce 89, “7” na stránce 89)**	MQZAO_SET_ ALL_CONTEXT	Nelze použít	MQZA_SET_ ALL_CONTEXT **(“6” na stránce 89)**

Tabulka 9. Autorizace zabezpečení potřebná pro volání MQOPEN (pokračování)			
Je vyžadována autorizace pro:	**Objekt fronty (“1” na stránce 88)**	**Objekt procesu**	**Objekt správce front**
MQOO_OUTPUT (Přenosová fronta) **(“8” na stránce 89)**	MQZAO_SET_ ALL_CONTEXT	Nelze použít	MQZA_SET_ ALL_CONTEXT **(“6” na stránce 89)**
MQOOK_SADA	MQZAO_SADA	Nelze použít	Žádná kontrola
MQO_ALTERNATE_ USER_AUTHORITY	**(“9” na stránce 89)**	**(“9” na stránce 89)**	MQZAO_ALTERNATE_ USER_AUTHORITY **(“9” na stránce 89, “10” na stránce 89)**

Tabulka 10. Autorizace zabezpečení potřebná pro volání MQPUT1			
Je vyžadována autorizace pro:	**Objekt fronty (“1” na stránce 88)**	**Objekt procesu**	**Objekt správce front**
KONTEXT MQPMO_PASS_ IDENTITY_CONTEXT	MQZA_PASS_ IDENTITY_CONTEXT **(“11” na stránce 89)**	Nelze použít	Žádná kontrola
MQPMO_PASS_ALL _CONTEXT	MQZA_PASS_ ALL_CONTEXT **(“11” na stránce 89)**	Nelze použít	Žádná kontrola
KONTEXT MQPMO_SET_ IDENTITY_CONTEXT	MQZA_SET_ IDENTITY_CONTEXT **(“11” na stránce 89)**	Nelze použít	MQZA_SET_ IDENTITY_CONTEXT **(“6” na stránce 89)**
MQPMO_SET_ ALL_CONTEXT	MQZA_SET_ ALL_CONTEXT **(“11” na stránce 89)**	Nelze použít	MQZA_SET_ ALL_CONTEXT **(“6” na stránce 89)**
(Přenosová fronta) **(“8” na stránce 89)**	MQZAO_SET_ ALL_CONTEXT	Nelze použít	MQZA_SET_ ALL_CONTEXT **(“6” na stránce 89)**
MQPMO_ALTERNATE_ USER_AUTHORITY	**(“12” na stránce 89)**	Nelze použít	MQZAO_ALTERNATE_ USER_AUTHORITY **(“10” na stránce 89)**

Tabulka 11. Autorizace zabezpečení potřebná pro volání MQCLOSE			
Je vyžadována autorizace pro:	**Objekt fronty (“1” na stránce 88)**	**Objekt procesu**	**Objekt správce front**
MQCO_DELETE	MQZAO_DELETE **(“13” na stránce 89)**	Nelze použít	Nelze použít
VYPRÁZDNIT ODSTRANĚNÍ MQCO_DELETE	MQZAO_DELETE **(“13” na stránce 89)**	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 89).
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.

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

Objekt	Je vyžadována autorizace
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
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 94)

Objekt	Je vyžadována autorizace
Fronta	MQZAO_CREATE **(“2” na stránce 94)**
Téma	MQZAO_CREATE **(“2” na stránce 94)**
Proces	MQZAO_CREATE **(“2” na stránce 94)**
Správce front	Nelze použít
Seznam názvů	MQZAO_CREATE **(“2” na stránce 94)**
Ověřovací informace	MQZAO_CREATE **(“2” na stránce 94)**
Kanál	MQZAO_CREATE **(“2” na stránce 94)**
Kanál připojení klienta	MQZAO_CREATE **(“2” na stránce 94)**
Modul listener	MQZAO_CREATE **(“2” na stránce 94)**
Služba	MQZAO_CREATE **(“2” na stránce 94)**
Informace o komunikaci	MQZAO_CREATE **(“2” na stránce 94)**

DEFINE *objekt* REPLACE (“1” na stránce 94, “3” na stránce 94)

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

Objekt	Je vyžadována autorizace
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
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

Příkaz	Objekt	Je vyžadována autorizace
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
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'	

Příkaz	Objekt	Je vyžadována autorizace
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, zadáním 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 *objekt* NOREPLACE.

Související informace

Klastrování: Využití doporučených postupů pro příkaz REFRESH CLUSTER

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 *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

Objekt	Je vyžadována autorizace
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
Kanál připojení klienta	Nelze použít
Modul listener	Nelze použít
Služba	Nelze použít
Informace o komunikaci	Nelze použít

Kopírování *objekt* (bez náhrady) (1)

Objekt	Je vyžadována autorizace
Fronta	MQZAO_CREATE **(2)**
Téma	MQZAO_CREATE **(2)**
Proces	MQZAO_CREATE **(2)**
Správce front	Nelze použít
Seznam názvů	MQZAO_CREATE **(2)**
Ověřovací informace	MQZAO_CREATE **(2)**
Kanál	MQZAO_CREATE **(2)**
Kanál připojení klienta	MQZAO_CREATE **(2)**
Modul listener	MQZAO_CREATE **(2)**
Služba	MQZAO_CREATE **(2)**
Informace o komunikaci	MQZAO_CREATE **(“2” na stránce 100)**

Kopírování *objekt* (s nahrazením) (1, 4)

Objekt	Je vyžadována autorizace
Fronta	ZMĚNA MQZAO_CHANGE

Objekt	Je vyžadována autorizace
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)**
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)**

Vytvořte *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

Objekt	Je vyžadována autorizace
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
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 objektu *objekt*

Objekt	Je vyžadována autorizace
Fronta	Žádná kontrola
Téma	Žádná kontrola
Proces	Žádná kontrola
Správce front	Žádná kontrola

Objekt	Je vyžadována autorizace
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
Ověřovací informace	Nelze použít
Kanál	MQZAO_CONTROL
Kanál připojení klienta	Nelze použít
Modul listener	MQZAO_CONTROL
Služba	MQZAO_CONTROL
Informace o komunikaci	Nelze použít

Zastavte *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
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'	
Reset klastru	Vyžadováno členství ve skupině 'mqm'	
Pozastavit klastr správců front	Vyžadováno členství ve skupině 'mqm'	
Obnovit klastr správců front	Vyžadováno členství ve skupině 'mqm'	

Další administrativní příkazy

Příkaz	Objekt	Je vyžadována autorizace
Odeslat signál Ping pro správce front	Správce front	MQZAO_ZOBRAZENÍ
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, zadáním 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.

Speciální aspekty zabezpečení v systému Windows

Některé funkce zabezpečení se chovají odlišně v různých verzích systému Windows.

Zabezpečení produktu IBM WebSphere MQ spoléhá na volání rozhraní API operačního systému na informace o autorizacích uživatele a členství ve skupinách. Některé funkce se v systémech Windows nechovají stejně. Tato kolekce témat zahrnuje popisy toho, jak tyto rozdíly mohou ovlivnit zabezpečení produktu IBM WebSphere MQ , když spouštíte produkt IBM WebSphere MQ v prostředí Windows .

Ukončovací program kanálu SSPI

Produkt WebSphere MQ for Windows poskytuje uživatelský program zabezpečení, který lze použít u zpráv i kanálů 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 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 podporovaných produktem WebSphere MQ verze 7.0.

Tato služba se obvykle používá v kanálu MQI k povolení správce front serveru k ověření identity aplikace klienta WebSphere MQ MQI. 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 WebSphere MQ verze 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 navzájem ověřovat totožnost správce front serveru a klientské aplikace WebSphere MQ MQI. 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.

Když obdržíte chybu 'group not found' v systému Windows

Tento problém může nastat, protože produkt WebSphere MQ ztratí přístup k lokální skupině mqm, jsou-li servery Windows povýšeny na řadiče domény nebo jsou z nich vyřazovány z provozu. Chcete-li tento problém odstranit, znovu vytvořte lokální skupinu mqm.

Příznakem je chyba označující nepřítomnost lokální skupiny mqm, například:

```
>crtmqm qm0
AMQ8066:Local mqm group not found.
```

Pozměnění stavu počítače mezi serverem a řadičem domény může ovlivnit provoz produktu WebSphere MQ, protože produkt WebSphere MQ používá lokálně definovanou skupinu 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.

Chcete-li tento problém odstranit, znovu vytvořte lokální skupinu mqm pomocí standardních nástrojů správy systému Windows . Protože jsou ztraceny všechny informace o členství ve skupině, je třeba znovu zavést privilegované uživatele produktu WebSphere MQ v nově vytvořené lokální skupině mqm. Je-li počítač členem domény, musíte také přidat skupinu mqm do lokální skupiny mqm, aby bylo možné udělit privilegovanou doménu WebSphere MQ ID požadované úrovně oprávnění.

Máte-li problémy s IBM WebSphere MQ a řadiči domény v systému Windows

Některé problémy mohou vyvstat v nastavení zabezpečení, když jsou servery Windows povýšeny na řadiče domény.

Při povýšení serverů Windows 2000, Windows 2003 nebo Windows Server 2008 na řadiče domény se zobrazí volba výběru výchozího nebo jiného než výchozího nastavení zabezpečení pro oprávnění uživatelů a skupin. Tato volba určuje, zda lze z aktivního adresáře načíst členství ve skupině (arbitrární). Vzhledem k tomu, že produkt WebSphere MQ spoléhá na informace o členství ve skupinách pro implementaci své zásady zabezpečení, je důležité, aby ID uživatele, které provádí operace produktu WebSphere MQ , určilo členství ostatních uživatelů ve skupinách.

Je-li v systému Windows 2000 vytvořena doména s použitím výchozí volby zabezpečení, výchozí ID uživatele vytvořené produktem WebSphere MQ během procesu instalace může podle potřeby získat členství ve skupinách pro ostatní uživatele. Produkt se pak instaluje normálně, vytváří výchozí objekty a správce front může v případě potřeby určit přístupové oprávnění lokálních a doménových uživatelů.

Je-li v systému Windows 2000 vytvořena doména s použitím jiné než výchozí volby zabezpečení nebo v systému Windows 2003 a Windows Server 2008, je-li doména vytvořena s použitím výchozí volby zabezpečení, ID uživatele vytvořené produktem WebSphere MQ během instalace nemůže vždy určit požadovaná členství ve skupině. V tomto případě byste měli vědět:

- Jak je operační systém Windows 2000 s nestandardním nastavením, nebo Windows 2003 a Windows Server 2008 s předvolbou zabezpečení, se chovají oprávnění zabezpečení
- Jak povolit členům skupiny domény mqm, aby přečetli členství ve skupině
- Jak nakonfigurovat službu IBM WebSphere MQ Windows tak, aby se spouštěla pod uživatelem domény.

Doména Windows 2000 s jinou než výchozí, nebo doména Windows 2003 a Windows Server 2008 s výchozími oprávněními zabezpečení

Instalace produktu WebSphere MQ se chová různě v těchto operačních systémech v závislosti na tom, zda lokální uživatel nebo uživatel domény provádí instalaci.

Pokud uživatel produktu **lokální** instaluje produkt WebSphere MQ, Průvodce přípravou produktu WebSphere MQ zjistí, že lokální uživatel vytvořený pro službu IBM WebSphere MQ Windows může načíst informace o členství ve skupině pro uživatele instalace. Průvodce přípravou produktu WebSphere MQ požádá uživatele o otázky o konfiguraci sítě, aby určil, zda jsou na řadičích domén spuštěných v systému Windows 2000 nebo novějším definovány jiné uživatelské účty. Je-li tomu tak, služba IBM WebSphere MQ Windows musí být spuštěna pod doménovým uživatelským účtem se zvláštním nastavením a oprávněními. Průvodce přípravou produktu WebSphere MQ vyzve uživatele k zadání podrobností o účtu tohoto uživatele. Jeho nápověda online poskytuje podrobnosti o požadovaném uživatelském účtu domény, který může být odeslán administrátorovi domény.

Pokud uživatel **doména** nainstaluje produkt WebSphere MQ, Průvodce přípravou produktu WebSphere MQ zjistí, že lokální uživatel vytvořený pro službu IBM WebSphere MQ Windows nemůže načíst informace o členství ve skupině pro uživatele s instalací. V tomto případě Průvodce přípravou produktu WebSphere MQ Wizard vždy vyzve uživatele k zadání podrobností o účtu uživatele domény pro službu IBM WebSphere MQ Windows , která má být použita.

Když služba IBM WebSphere MQ Windows potřebuje použít uživatelský účet domény, produkt WebSphere MQ nemůže pracovat správně, dokud nebude konfigurován pomocí Průvodce přípravou produktu WebSphere MQ . Průvodce přípravou produktu WebSphere MQ neumožní uživateli pokračovat s dalšími úlohami, dokud nebude služba Windows konfigurována s vhodným účtem.

Pokud byla doména systému Windows 2000 nakonfigurována s použitím jiných než výchozích oprávnění zabezpečení, je běžné řešení pro správnou funkci produktu WebSphere MQ správně fungovat s odpovídajícím uživatelským účtem domény, jak je popsáno výše.

Další informace naleznete v tématu Vytvoření a nastavení doménových účtů pro produkt WebSphere MQ .

Konfigurace služeb produktu IBM WebSphere MQ pro spuštění pod uživatelem domény v systému Windows
Pomocí průvodce přípravou produktu IBM WebSphere MQ zadejte podrobnosti o účtu pro uživatelský účet domény. Případně můžete použít panel Správa počítačů ke změně podrobností **Přihlášení** pro konkrétní službu produktu IBM WebSphere MQ pro instalaci.

Další informace viz téma Změna hesla uživatelského účtu služby IBM WebSphere MQ Windows

Použití souborů šablon zabezpečení v systému Windows

Použití šablony může ovlivnit nastavení zabezpečení aplikované na soubory a adresáře produktu WebSphere MQ . Používáte-li vysoce zabezpečenou šablonu, použijte ji před instalací produktu WebSphere MQ.

Systém Windows podporuje soubory šablon zabezpečení založených na textu, které můžete použít k použití uniformních nastavení zabezpečení pro jeden nebo více počítačů pomocí modulu snap-in Konfigurace zabezpečení a analýzy MMC. Systém Windows poskytuje zejména několik šablon, které zahrnují celou řadu nastavení zabezpečení s cílem poskytovat specifické úrovně zabezpečení. Tyto šablony zahrnují Kompatibilní, Zabezpečené a Vysoce zabezpečené.

Použití jedné z těchto šablon může ovlivnit nastavení zabezpečení aplikované na soubory a adresáře produktu WebSphere MQ . Chcete-li použít šablonu Highly Secure, nakonfigurujte počítač před instalací produktu WebSphere MQ.

Pokud použijete vysoce zabezpečenou šablonu na počítač, na kterém je produkt WebSphere MQ již nainstalován, budou odebrána všechna oprávnění, která jste nastavili na souborech a adresářích produktu WebSphere MQ . Protože tato oprávnění jsou odebrána, ztratíte uživatele *Administrator*, *mqm*a v případě potřeby přístup skupiny *Everyone* z chybových adresářů.

Vnořené skupiny

Pro použití vnořených skupin existují omezení. Tyto výsledky částečně pocházejí z funkční úrovně domény a částečně z omezení produktu WebSphere MQ .

Volba Active Directory může podporovat různé typy skupin v rámci kontextu domény v závislosti na funkční úrovni domény. Ve výchozím nastavení jsou domény systému Windows 2003 na funkční úrovni *Windows 2000 mixed* . (Windows server 2003, Windows XP, Windows Vista a Windows Server 2008 se všechny řídí modelem 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 pro ID používaná produktem WebSphere MQ. Síťová rozhraní API používaná produktem WebSphere MQ nepodporují všechny konfigurace, které jsou podporovány funkční úrovní domény. Výsledkem je, že produkt WebSphere MQ nemůže zadat dotaz na členství ve skupině všech ID domén existujících 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.

Konfigurace dalšího oprávnění pro aplikace Windows , které se připojují k produktu IBM WebSphere MQ

Účet, pod kterým mohou být spuštěny procesy produktu IBM WebSphere MQ , může potřebovat další oprávnění před tím, než může být udělen přístup k procesům SYNCHRONIZE k aplikačním procesům.

Mohou se vyskytnout problémy, pokud máte aplikace systému Windows , například stránky ASP, připojení k serveru IBM WebSphere MQ , které jsou konfigurovány pro spuštění na úrovni zabezpečení vyšší, než je obvyklé.

IBM WebSphere MQ vyžaduje přístup SYNCHROIZE k procesům aplikace za účelem koordinace určitých akcí. APAR IC35116 změnil IBM WebSphere MQ tak, že jsou uvedena příslušná oprávnění. Avšak účet, pod kterým jsou spuštěny procesy produktu IBM WebSphere MQ , může vyžadovat další oprávnění, dříve než může být udělen požadovaný přístup.

Když se serverová aplikace nejprve pokusí o připojení ke správci front, IBM WebSphere MQ upraví proces tak, aby udělil oprávnění SYNCHRONIZE pro administrátory produktu IBM WebSphere MQ . Chcete-li konfigurovat další oprávnění k ID uživatele, pod kterým jsou procesy produktu IBM WebSphere MQ spuštěny, postupujte takto:

1. Spusťte nástroj Lokální zásada zabezpečení, klepněte na Nastavení zabezpečení-> Lokální zásady-> Uživatelská práva, klepněte na "Ladit programy".
2. Poklepejte na "Ladicí programy" a potom do seznamu přidejte ID uživatele produktu IBM WebSphere MQ

Je-li systém v doméně systému 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.

Nastavení zabezpečení v systému HP Integrity NonStop Server

Aspekty zabezpečení specifické pro systémy HP Integrity NonStop Server .

Klient IBM WebSphere MQ pro produkt HP Integrity NonStop Server podporuje při připojování ke správci front protokol TLS (Transport Layer Security) a SSL (Secure Sockets Layer) k zajištění zabezpečení na úrovni propojení. Tyto protokoly jsou podporovány pomocí implementace OpenSSL. OpenSSL vyžaduje zdroj náhodných dat pro poskytování silných šifrovacích operací.

OpenSSL

Přehled zabezpečení OpenSSL pro klienta IBM WebSphere MQ pro produkt HP Integrity NonStop Server.

Sada nástrojů OpenSSL je implementací zabezpečení SSL (Secure Sockets Layer) a TLS (Transport Layer Security) pro zabezpečenou komunikaci po síti.

Tuto sadu nástrojů vyvíjí projekt OpenSSL Project. Další informace o projektu OpenSSL Project viz https://www.openssl.org. Klient produktu IBM WebSphere MQ for HP Integrity NonStop Server obsahuje upravené verze knihoven OpenSSL a příkazu **openssl** . Knihovny a příkaz **openssl** jsou portovány z sady nástrojů OpenSSL 1.0.1ca jsou dodávány pouze jako kód objektu. Není poskytnut žádný zdrojový kód.

Knihovny OpenSSL jsou podle potřeby zaváděné klientskými aplikačními programy klienta IBM WebSphere MQ . Pro použití s klientskými aplikacemi produktu IBM WebSphere MQ jsou podporovány pouze knihovny OpenSSL , které jsou poskytovány produktem IBM WebSphere MQ .

Příkaz **openssl** , který může být použit pro účely správy certifikátů, je nainstalován v adresáři OSS `opt_installation_path/opt/mqm/bin`.

Pomocí příkazu **openssl** můžete vytvářet a spravovat klíče a digitální certifikáty s různými běžnými formáty dat a provádět jednoduché úlohy certifikační autority (CA).

Výchozí formát pro data klíče a certifikátu, který je zpracován OpenSSL , je formát PEM (Privacy Enhanced Mail). Data ve formátu PEM jsou data ASCII kódovaná ve formátu base64 . Data lze proto přenášet pomocí textově založených systémů, jako je e-mail, a lze je pomocí textových editorů a webových prohlížečů vkládat a vkládat. PEM je internetovým standardem pro kryptografické výměny šifrovaného textu a je specifikován v internetových RFC 1421, 1422, 1423 a 1424. IBM WebSphere MQ předpokládá, že soubor s příponou `.pem` obsahuje data ve formátu PEM. Soubor ve formátu PEM může obsahovat více certifikátů a jiných kódovaných objektů a může obsahovat komentáře.

Podpora zabezpečení SSL serveru IBM WebSphere MQ v jiných operačních systémech může vyžadovat data klíče a certifikátu v souborech, které mají být zakódovány pomocí DER (Distinguished Encoding Rules). DER je sada pravidel kódování pro použití notace ASN.1 v zabezpečené komunikaci. Data kódovaná pomocí DER jsou binární data a formát klíče a dat certifikátu kódovaný pomocí DER je také známý jako PKCS#12 nebo PFX. Soubor, který obsahuje tato data, má obvykle příponu `.p12` nebo `.pfx`. Příkaz **openssl** lze převést mezi formátem PEM a PKCS#12 .

Démon entropie

OpenSSL vyžaduje zdroj náhodných dat pro poskytování silných šifrovacích operací. Generování náhodného čísla je funkce, která je obvykle poskytována operačním systémem nebo procesem démona v rámci celého systému. Operační systém HP Integrity NonStop Server tuto schopnost v rámci operačního systému neposkytuje.

Pokud používáte podporu zabezpečení SSL a TLS dodávané s klientem produktu IBM WebSphere MQ pro produkt HP Integrity NonStop Server, je nutný proces, který se nazývá entropie démon, aby poskytl zdroj náhodných dat. Když spustíte kanál klienta, který vyžaduje SSL nebo TLS, OpenSSL očekává, že démon entropie bude spuštěn a poskytuje své služby na soketu v systému souborů OSS v `/etc/egd-pool`.

Démon entropie není poskytován klientem IBM WebSphere MQ pro HP Integrity NonStop Server. Klient IBM WebSphere MQ pro HP Integrity NonStop Server je testován s následujícími entropy démony:

- amqjkdm0 (jak je poskytováno serverem IBM WebSphere MQ 5.3)
- `/usr/local/bin/prngd` (verze 0.9.27, jak je poskytována produktem HP Integrity NonStop Server Open Source Technical Library)

Nastavení zabezpečení klienta IBM WebSphere MQ MQI

Je třeba zvážit zabezpečení klienta IBM WebSphere MQ MQI, 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.

  Měli byste použít vzájemné ověření v rámci SSL nebo TLS. Další informace naleznete v tématu “Práce s SSL nebo TLS” na stránce 108
- 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 155.

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 uživatelem deklarovaného ID uživatele na ID uživatele MCAUSER” na stránce 181.

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 39.

Určení, že pro běhové prostředí klienta MQI je použit pouze certifikovaný standard FIPS CipherSpecs

Vytvořte svá úložiště klíčů pomocí softwaru vyhovujícího standardu FIPS a poté zadejte, že kanál musí používat certifikovanou FIPS CipherSpecs.

Má-li být úložiště klíčů kompatibilní se standardem FIPS za běhu, musí být vytvořena a spravována pouze softwarem vyhovujícím FIPS, jako je runmqakm s volbou -fips.

Můžete určit, že kanál zabezpečení SSL nebo TLS musí ve třech ohledech používat pouze certifikovaný standard FIPS CipherSpecs , a to v pořadí podle priority:

1. Nastavte pole FipsRequired ve struktuře MQSCO pro MQSSL_FIPS_YES.
2. Nastavte proměnnou prostředí MQSSLFIPS na hodnotu YES.
3. Nastavte atribut SSLFipsRequired v konfiguračním souboru klienta na hodnotu YES.

Ve výchozím nastavení není certifikovaná FIPS CipherSpecs vyžadována.

Tyto hodnoty mají stejný význam jako ekvivalentní hodnoty parametrů v příkazu ALTER QMGR SSLFIPS (viz ALTER QMGR). Pokud proces klienta aktuálně nemá žádné aktivní připojení SSL nebo TLS a hodnota FipsRequired je na zabezpečení SSL MQCONNX platně zadána, všechny následné připojení SSL přidružené k tomuto procesu musí používat pouze CipherSpecs přidružené k této hodnotě. To platí, dokud se nezastavily všechny ostatní připojení SSL nebo TLS, v tom případě může další vlastnost MQCONNX poskytnout novou hodnotu pro FipsRequired.

Je-li nainstalován kryptografický hardware, mohou být kryptografické moduly používané produktem WebSphere MQ konfigurovány tak, aby byly moduly poskytované hardwarovým produktem, a tyto moduly mohou být certifikovány FIPS na konkrétní úroveň. Konfigurovatelné moduly a informace o tom, zda jsou certifikovány FIPS, závisí na použití hardwarového produktu.

Je-li to možné, v případě, že je konfigurován pouze standard FIPS CipherSpecs , pak klient MQI odmítne připojení, která specifikují non-FIPS CipherSpec s MQRC_SSL_INITIALIZATION_ERROR. Produkt WebSphere MQ nezaručuje odmítnutí všech takových připojení a je vaší odpovědností určit, zda je vaše konfigurace produktu WebSphere MQ kompatibilní se standardem FIPS-.

Související pojmy

“Standard FIPS (Federal Information Processing Standards) pro systémy UNIX, Linuxa Windows” na stránce 25

Je-li vyžadováno šifrování v kanálu SSL nebo TLS v systémech Windows, UNIX and Linux používá produkt WebSphere MQ šifrovací balík s názvem IBM Crypto for C (ICC). Na platformách Windows, UNIX and Linux 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.

stanza SSL konfiguračního souboru klienta

Související odkazy

FipsRequired (MQLONG)

MQSSLFIPS

Spouštění aplikací klienta SSL nebo TLS s více instalacemi sady GSKit V8.0 na systému AIX

Při spuštění na systémech AIX s více instalacemi sady GSKit V8.0 se mohou klientské aplikace SSL nebo TLS v produktu AIX setkat s produktem MQRC_CHANNEL_CONFIG_ERROR a chybou AMQ6175 .

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 SSL nebo 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 WebSphere MQ zaváděl smíšenou sadu knihoven ze dvou různých instalací sady GSKit V8.0 . Provedení této chyby může způsobit provedení klientské aplikaceIBM WebSphere MQ v prostředí Db2 .

Chcete-li se této chybě vyhnout, zahrňte do cesty ke knihovně adresáře knihovny IBM WebSphere MQ , aby měly knihovny IBM WebSphere MQ přednost. Toho lze dosáhnout pomocí příkazu **setmqenv** s parametrem **-k** , například:

```
. /usr/mqm/bin/setmqenv -s -k
```

Další informace o použití příkazu **setmqenv** najdete v souboru setmqenv (nastavení prostředí WebSphere MQ)

Nastavení komunikace pro zabezpečení SSL nebo TLS v systémech UNIX, 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 systémech UNIX, Linux a Windows můžete provádět testy s certifikáty s vlastním podpisem.

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 se SSL nebo TLS na systémech UNIX, Linux, and Windows” na stránce 111.

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 WebSphere MQ server SSL nebo TLS vždy požaduje certifikát od klienta.

V systémech UNIX, Linux a Windows odešle klient SSL nebo TLS certifikát pouze v případě, že má jeden označený ve správném formátu IBM WebSphere 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 WebSphere MQ je `ibmwebspheremq` následováno vaším přihlašovacím ID uživatele změněno na malá písmena, například `ibmwebspheremqmyuserid`.

IBM WebSphere 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 viz “Připojení dvou správců front s použitím zabezpečení SSL nebo TLS” na stránce 201.

Práce s SSL nebo TLS

Tato témata obsahují pokyny pro provádění jednotlivých úloh souvisejících s používáním SSL nebo TLS s produktem IBM WebSphere MQ.

Mnoho z nich se používá jako kroky v úlohách vysoké úrovně popsaných v následujících sekcích:

- “Identifikace a ověřování uživatelů” na stránce 141
- “Autorizace přístupu k objektům” na stránce 155
- “Důvěrnost zpráv” na stránce 201
- “Integrita dat zpráv” na stránce 222
- “Uchování zabezpečených klastrů” na stránce 239

Práce s SSL nebo TLS v systému HP Integrity NonStop Server

Popisuje klienta IBM WebSphere MQ pro implementaci zabezpečení produktu HP Integrity NonStop Server OpenSSL včetně služeb zabezpečení, komponent, podporovaných verzí protokolu, podporovaných specifikací CipherSpecsa nepodporovaných funkcí zabezpečení.

Podpora zabezpečení SSL & TLS produktu IBM WebSphere MQ poskytuje následující služby zabezpečení pro kanály klienta:

- Ověřování serveru a volitelně i ověření klienta.
- Šifrování a dešifrování dat, která proudí přes kanál.
- Integrita kontroluje data, která proudí přes kanál.

Podpora zabezpečení SSL a TLS dodávaná s klientem produktu IBM WebSphere MQ pro produkt HP Integrity NonStop Server se skládá z následujících komponent:

- Knihovny OpenSSL a příkaz **`openssl`** .
- Příkaz pro uložení hesla produktu IBM WebSphere MQ , **`amqrsslc`**.

Následující vyžadované komponenty pro operaci kanálu klienta SSL nebo TLS nejsou poskytnuty s klientem IBM WebSphere MQ pro produkt HP Integrity NonStop Server:

- Démon entropie, který poskytuje zdroj náhodných dat pro šifrování OpenSSL .

Podporované verze protokolu

Klient IBM WebSphere MQ for HP Integrity NonStop Server podporuje následující verze protokolu:

- SSL 3.0
- TLS 1.0
- TLS 1.2

Podporované CipherSpecs

Klient IBM WebSphere MQ for HP Integrity NonStop Server podporuje následující verze CipherSpecs :

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- RC4_SHA_US
- RC4_MD5_US
- TRIPLE_DES_SHA_US
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (zamítnuto)
- DES_SHA_EXPORT1024
- RC4_56_SHA_EXPORT1024
- RC4_MD5_EXPORT
- RC2_MD5_EXPORT
- DES_SHA_EXPORT
- TLS_RSA_WITH_DES_CBC_SHA
- NULL_SHA
- NULL_MD5
- FIPS_WITH_DES_CBC_SHA
- FIPS_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_NULL_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- ECDHE_ECDSA_AES_128_CBC_SHA256
- ECDHE_ECDSA_AES_256_CBC_SHA384
- ECDHE_RSA_AES_128_CBC_SHA256
- ECDHE_RSA_AES_256_CBC_SHA384
- ECDHE_ECDSA_AES_128_GCM_SHA256
- ECDHE_ECDSA_AES_256_GCM_SHA384
- ECDHE_RSA_AES_128_GCM_SHA256
- ECDHE_RSA_AES_256_GCM_SHA384

Nepodporovaná funkce zabezpečení

Klient IBM WebSphere MQ for HP Integrity NonStop Server v současné době nepodporuje:

- PKCS#11 Podpora kryptografického hardwaru
- Kontrola seznamu odvolaných certifikátů LDAP
- Kontrola protokolu OCSP online certifikátů

- FIPS 140-2, řídicí prvky šifrovací sady NSA SUITE B

Správa certifikátů

K uložení digitálního certifikátu a informací o odvolaných certifikátech použijte sadu souborů.

Podpora SSL a TLS produktu IBM WebSphere MQ používá sadu souborů k ukládání digitálního certifikátu a informací o odvolaných certifikátech. Tyto soubory jsou umístěny v adresáři určeném buď programově pomocí pole KeyRepository ve struktuře MQSCO předané na volání MQCONNX, pomocí proměnné prostředí *MQSSLKEYR* , nebo ve stanze SSL v produktu `mqclient.ini` pomocí atributu SSLKeyRepository .

Struktura MQSCO má přednost před proměnnou prostředí MQSSLKEYR, která má přednost před hodnotou sekce ini souboru.

Důležité: Umístění úložiště klíčů uvádí umístění adresáře a ne název souboru na platformě HP Integrity NonStop Server .

Klient IBM WebSphere MQ pro produkt HP Integrity NonStop Server používá následující citlivé soubory s názvy souborů v umístění úložiště klíčů:

- "Úložiště osobních certifikátů" na stránce 110
- "Důvěryhodnost certifikátu" na stránce 110
- "Předat soubor pro uložení fráze" na stránce 111
- "Soubor se seznamem odvolaných certifikátů" na stránce 111

Úložiště osobních certifikátů
Soubor osobního úložiště certifikátů, `cert.pem`.

Tento soubor obsahuje osobní certifikát a zašifrovaný soukromý klíč klienta, který se má použít, ve formátu PEM. Existence tohoto souboru je volitelná, pokud používáte kanál SSL nebo TLS, které nevyžadují autentizaci klienta. Je-li u kanálu vyžadováno ověření klienta a SSLCAUTH (POVINNÝ) je zadán v definici kanálu, tento soubor musí existovat a musí obsahovat jak certifikát, tak šifrovaný soukromý klíč.

Chcete-li povolit přístup pro čtení k vlastníkovi úložiště certifikátů, musí být na tomto souboru nastavena oprávnění k souboru.

Správně formátovaný soubor `cert.pem` musí obsahovat přesně dvě sekce s následujícími záhlavími a zápatími:

```
-----BEGIN PRIVATE KEY-----
Base 64 ASCII encoded private key data here
-----END PRIVATE KEY-----
```

```
-----BEGIN CERTIFICATE-----
Base 64 ASCII encoded certificate data here
-----END CERTIFICATE-----
```

Fráze hesla pro šifrovaný soukromý klíč je uložena v souboru pro uložení frází schválení `Stash.sth`.

Důvěryhodnost certifikátu
Soubor úložiště údajů o důvěryhodnosti certifikátu `trust.pem`.

Tento soubor obsahuje certifikáty potřebné k ověření osobních certifikátů, které používají správci front, ke kterým se klient připojuje, ve formátu PEM. Úložiště údajů o důvěryhodnosti certifikátu je povinné pro všechny kanály klienta SSL nebo TLS.

Pro omezení přístupu k zápisu do tohoto souboru musí být nastavena oprávnění k souboru.

Správně formátovaný soubor `trust.pem` musí obsahovat jednu nebo více sekcí s následujícími záhlavími a zápatími:

```
-----BEGIN CERTIFICATE-----
Base 64 ASCII encoded certificate data here
-----END CERTIFICATE-----
```

Předat soubor pro uložení fráze
Soubor stash Fráze stash, `Stash.sth`.

Tento soubor je binárním formátem soukromým pro IBM WebSphere MQ a obsahuje šifrovanou frázi hesla pro použití při přístupu k soukromému klíči, který je uložen v souboru `cert.pem` . Samotný soukromý klíč je uložen v úložišti certifikátů produktu `cert.pem` .

Tento soubor je vytvořen nebo změněn pomocí nástroje příkazového řádku IBM WebSphere MQ **amqrsslc** s parametrem **-s** . Například, kde adresář `/home/alice` obsahuje soubor `cert.pem` :

```
amqrsslc -s /home/alice/cert

  Enter password for Keystore /home/alice/cert.pem :
    password

  Stashed the password in file /home/alice/Stash.sth
```

Chcete-li povolit přístup pro čtení k vlastníkovi přidruženého úložiště osobních certifikátů, musí být na tomto souboru nastavena oprávnění k souboru.

Soubor se seznamem odvolaných certifikátů
Soubor se seznamem odvolaných certifikátů `crl.pem`.

Tento soubor obsahuje seznam odvolaných certifikátů (CRL), který klient používá k ověření digitálních certifikátů ve formátu PEM. Existence tohoto souboru je volitelná. Není-li tento soubor k dispozici, při ověřování certifikátů nejsou provedeny žádné kontroly odvolání certifikátů.

Pro omezení přístupu k zápisu do tohoto souboru musí být nastavena oprávnění k souboru.

Správně formátovaný soubor `crl.pem` musí obsahovat jednu nebo více sekcí s následujícími záhlavími a zápatími:

```
-----BEGIN X509 CRL-----
Base 64 ASCII encoded CRL data here
-----END X509 CRL-----
```

Práce se SSL nebo TLS na systémech UNIX, Linux, and Windows

V systémech UNIX, Linux a Windows je podpora zabezpečení SSL (Secure Sockets Layer) instalována s produktem IBM WebSphere MQ.

Podrobnější informace o zásadách ověření platnosti certifikátu naleznete v tématu Ověřování platnosti certifikátu a návrh zásad důvěryhodnosti.

Použití iKeyman, iKeycmd, runmqakm a runmqckm

V systémech UNIX, Linux a Windows spravujte klíče a digitální certifikáty pomocí rozhraní GUI iKeyman nebo z příkazového řádku pomocí příkazu iKeycmd nebo runmqakm.

- Pro systémy **UNIX and Linux** :
  - Ke spuštění grafického uživatelského rozhraní iKeyman použijte příkaz **strmqikm** .
  - Příkaz **runmqckm** se používá k provádění úloh s rozhraním příkazového řádku iKeycmd .
  - Příkaz **runmqakm** se používá k provádění úloh s rozhraním příkazového řádku runmqakm. Syntaxe příkazu pro **runmqakm** je stejná jako syntaxe pro **runmqckm**.

    Potřebujete-li spravovat certifikáty SSL 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, uvědomte si, že iKeycmd a iKeyman jsou 64bitové programy. Externí moduly vyžadované podporou PKCS #11 se načtou do 64bitového procesu, a proto musíte mít pro administraci na šifrovacím hardwaru nainstalovanou

64bitovou knihovnu PKCS #11. 32bitové platformy Windows a Linux x86 jsou jedinými výjimkami, protože programy iKeyman a iKeycmd jsou na těchto platformách 32 bitové.

Na následujících platformách, kde prostředí JRE bylo 32 bitů ve starších verzích produktu, ale je 64bitový pouze v produktu IBM WebSphere MQ Version 7.5, může být zapotřebí instalovat další ovladače PKCS#11 vhodné pro režim adresování prostředí JRE **iKeyman** a **iKeycmd** . Důvodem je to, že ovladač PKCS#11 musí používat stejný režim adresování jako prostředí JRE. V následující tabulce jsou uvedeny režimy adresování prostředí JRE produktu IBM WebSphere MQ Version 7.5 .

Tabulka 12. IBM WebSphere MQ Version 7.5 Režimy adresování JRE

Platforma	**Režim adresování JRE**
Windows (32 bitů nebo 64 bitů)	32
Linux pro System x 32 bitů	32
Linux pro System x 64 bitů	64
Linux pro System p	64
Linux pro System z	64
HP-UX	64
Solaris Sparc	64
Solaris x86-64	64
AIX	64

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
```

- Pro systémy **Windows** :
  – Ke spuštění grafického uživatelského rozhraní iKeyman použijte příkaz **strmqikm** .
  – Příkaz **runmqckm** se používá k provádění úloh s rozhraním příkazového řádku iKeycmd .

    Potřebujete-li spravovat certifikáty SSL způsobem, který vyhovuje standardu FIPS, použijte namísto příkazů **runmqckm** nebo **strmqikm** příkaz **runmqakm** .

Chcete-li vyžádat trasování SSL v systémech UNIX, Linux nebo Windows , prohlédněte si soubor strmqtrc.

Související odkazy
runmqckm a příkazy runmqakm

Nastavení úložiště klíčů v systémech UNIX, Linux, and Windows

Úložiště klíčů můžete nastavit pomocí uživatelského rozhraní iKeyman , nebo pomocí příkazů **iKeycmd** nebo **runmqakm** .

Informace o této úloze

Připojení SSL nebo TLS vyžaduje *úložiště klíčů* na každém konci připojení. Každý správce front produktu IBM WebSphere MQ a produkt IBM WebSphere MQ MQI client musí mít přístup k úložišti klíčů. Další informace viz “Úložiště klíčů SSL nebo TLS” na stránce 23.

Na systémech UNIX, Linux, and Windows jsou digitální certifikáty uloženy v souboru databáze klíčů, který je spravován pomocí uživatelského rozhraní produktu **iKeyman** , nebo pomocí příkazů **iKeycmd** nebo **runmqakm** . Tyto digitální certifikáty mají štítky. Specifický popisek asociuje osobní certifikát se správcem front nebo produktem IBM WebSphere MQ MQI client. SSL a TLS používají tento certifikát pro účely autentizace. Na systémech UNIX, Linux, and Windows produkt IBM WebSphere MQ používá `ibmwebspheremq` jako předponu štítku, aby nedošlo k záměně s certifikáty pro jiné produkty. Za předponou následuje název správce front nebo přihlašovací ID uživatele produktu IBM WebSphere MQ MQI client , který byl změněn na malá písmena. Ujistěte se, že jste zadali celé návěští certifikátu malými písmeny.

Název souboru databáze klíčů se skládá z cesty a názvu kmene:

- V systémech UNIX and Linux je výchozí cesta pro správce front (nastavená při vytvoření správce front) `/var/mqm/qmgrs/<queue_manager_name>/ssl`.

  Na systémech Windows je výchozí cesta *MQ_INSTALLATION_PATH*`\Qmgrs\`*queue_manager_name*`\ssl`, kde *MQ_INSTALLATION_PATH* je adresář, ve kterém je nainstalován produkt IBM WebSphere MQ . Například `C:\program files\IBM\WebSphere 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 WebSphere 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 systémech UNIX, Linux nebo Windows” na stránce 117 . Název souboru databáze klíčů můžete zadat buď před vytvořením databázového souboru klíčů, nebo po něm.

ID uživatele, ze kterého spouštíte příkazy **iKeyman** nebo **iKeycmd** , 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 **iKeyman** nebo **iKeycmd** , členem skupiny mqm. Pokud pro IBM WebSphere MQ MQI clientspustíte **iKeyman** nebo **iKeycmd** z ID uživatele odlišného od ID uživatele, pod kterým je klient spuštěn, musíte změnit oprávnění k souboru, aby mohl produkt IBM WebSphere MQ MQI client přistupovat k souboru databáze klíčů za běhu. Další informace viz “Přístup k databázovým souborům a jejich zabezpečení v systému Windows” na stránce 115 nebo “Přístup k databázovým souborům a jejich zabezpečení v systémech UNIX and Linux” na stránce 115.

V produktu **iKeyman** nebo **iKeycmd** verze 7.0jsou nové databáze klíčů automaticky naplněny sadou předem definovaných certifikátů certifikačních autorit (CA). V produktu **iKeyman** nebo **iKeycmd** verze 8.0nejsou databáze klíčů automaticky naplněny daty, takže počáteční nastavení je bezpečnější, protože do souboru databáze klíčů zahrnete pouze ty certifikáty CA, které chcete.

Poznámka: Kvůli této změně chování pro sadu GSKit verze 8.0 , která má za následek automatické přidávání certifikátů CA do úložiště, je třeba ručně přidat upřednostňované certifikáty CA. Tato změna chování vám poskytuje přesnější a detailnější kontrolu nad použitními certifikáty CA. Viz “Přidání výchozích certifikátů CA do prázdného úložiště klíčů v systémech UNIX, Linux, and Windows se sadou GSKit verze 8.0” na stránce 116.

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:
   - Na systémech UNIX, Linux, and Windows:

     ```
     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 produkt IBM WebSphere MQmusí být cms.)

   -stash
   Uloží heslo databáze klíčů do souboru.

   -fips
   Zakáže použití šifrovací knihovny BSafe. Použije se pouze komponenta ICC a tato komponenta musí být úspěšně inicializována 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 znakovém znakovém souboru ASCII v rozsahu 0x20 - 0x7E.

Volitelně můžete vytvořit databázi klíčů pomocí uživatelského rozhraní produktu **strmqikm** (iKeyman).

2. V systémech UNIX and Linux se přihlaste jako uživatel root. V systému Windows se přihlaste jako administrátor nebo jako člen skupiny MQM.
3. Spusťte uživatelské rozhraní iKeyman 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 UNIX and Linux) nebo `C:\Program Files\IBM\WebSphere MQ\qmgrs\QM1\ssl` (v systémech Windows).

     Cesta se musí shodovat s hodnotou atributu **SSLKeyRepository** správce front.
   - Pro klienta IBM WebSphere MQ : `/var/mqm/ssl` (v systémech UNIX and Linux) nebo `C:\mqm\ssl` (v systémech Windows).
8. Klepněte na tlačítko **Otevřít**.

   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 SSL nebo 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 115 nebo “Přístup k databázovým souborům a jejich zabezpečení v systémech UNIX and Linux” na stránce 115.

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*`.crl`a *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.

Přístup k databázovým souborům a jejich zabezpečení v systémech UNIX 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 -----).

Přidání výchozích certifikátů CA do prázdného úložiště klíčů v systémech UNIX, Linux, and Windows se sadou GSKit verze 8.0
Chcete-li přidat jeden nebo více výchozích certifikátů CA do prázdného úložiště klíčů s verzí 8 sady GSKit, postupujte podle této procedury.

V sadě GSKit verze 7.0se chování při vytváření nového úložiště klíčů mělo automaticky přidat do sady výchozích certifikátů CA pro běžně používaná certifikační autority. U sady GSKit verze 8 se 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 správce klíčů iKeyman

Níže uvedené kroky proveďte na počítači, na který chcete přidat certifikát CA:

1. Spusťte grafické uživatelské rozhraní iKeyman pomocí příkazu **strmqikm** (na systémech UNIX, Linux a 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 si přejete důvěřovat, abyste zobrazili úplný seznam platných certifikátů CA.
11. Vyberte certifikáty CA, které chcete důvěřovat ze seznamu, a klepněte na tlačítko **OK**. Certifikáty se přidají do úložiště klíčů.

z příkazového řádku,

Pomocí následujících příkazů zobrazte seznam a poté přidejte certifikáty CA pomocí příkazu iKeycmd:

- 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 v produktu WebSphere MQ důvěřuje všem osobním certifikátům podepsaným daným certifikátem CA. Zvažte pečlivě, 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.

Vyhledání úložiště klíčů pro správce front v systémech UNIX, 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 programu IBM WebSphere MQ Explorer nebo PCF.
2. Prověřte výstup příkazu pro cestu a název stem databázového souboru klíčů.
   Například
   a. na systémech UNIX and Linux : `/var/mqm/qmgrs/QM1/ssl/key`, kde `/var/mqm/qmgrs/QM1/ssl` je cesta a `key` je název kmene
   b. v systému 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, do kterého je produkt WebSphere MQ nainstalován.

Změna umístění úložiště klíčů pro správce front v systémech UNIX, Linux nebo 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 na systémech UNIX 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\WebSphere MQ\Qmgrs\QM1\ssl\Mykey')
```

Soubor databáze klíčů má úplný název souboru: `C:\Program Files\IBM\WebSphere 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 WebSphere 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 systémech UNIX, Linux, and Windows” na stránce 130.

Vyhledání úložiště klíčů pro klienta IBM WebSphere MQ MQI na systémech UNIX, Linux, and Windows

Umístění úložiště klíčů je dáno proměnnou MQSSLKEYR nebo zadanou v rámci volání MQCONNX.

Examine the MQSSLKEYR environment variable to obtain the location of your IBM WebSphere MQ MQI client's key database file. 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 klienta IBM WebSphere MQ MQI v systémech UNIX, Linux, and Windows” na stránce 118. Hodnota nastavená ve volání MQCONNX přepíše hodnotu proměnné MQSSLKEYR.

Určení umístění úložiště klíčů pro klienta IBM WebSphere MQ MQI v systémech UNIX, Linux, and Windows

Pro klienta IBM WebSphere MQ MQI neexistuje 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 klienta IBM WebSphere MQ MQI lze určit jedním z následujících dvou způsobů:

- Nastavení proměnné prostředí MQSSLKEYR. Například na systémech UNIX 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\WebSphere MQ\ssl\key
  ```

  Soubor databáze klíčů má plně kvalifikovaný název souboru:

  ```
  C:\Program Files\IBM\WebSphere 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 .

Když se změny certifikátů nebo paměti certifikátů stanou účinnými na systémech UNIX, Linux nebo 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:

- Při prvním spuštění kanálu s jedním kanálem se spustí kanál SSL.
- Při prvním přijetí požadavku na spuštění kanálu SSL má nový příchozí proces s jedním kanálem TCP/IP.
- Je-li příkaz MQSC REFRESH SECURITY TYPE (SSL) zadán k aktualizaci prostředí MQ SSL produktu WebSphere MQ.

- Pro procesy klientské aplikace, když je zavřeno poslední připojení SSL v procesu. Další připojení SSL 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 SSL. Pokud proces sdružování procesu již spustil kanál SSL a vy chcete, aby se změna stala efektivní okamžitě, 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 je spuštěn kanál SSL. Pokud proces iniciátoru kanálu již spustil kanál SSL a vy chcete, aby se změna stala efektivní 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 SSL. Pokud modul listener již spustil kanál SSL a chcete, aby se změny projevily okamžitě, spusťte příkaz MQSC REFRESH SECURITY TYPE (SSL).

Můžete také aktualizovat prostředí WebSphere MQ SSL pomocí příkazů programu IBM WebSphere MQ Explorer nebo PCF.

Vytvoření osobního certifikátu s automatickým podpisem na systémech UNIX, Linux, and Windows

Certifikát s automatickým podpisem můžete vytvořit pomocí skriptu iKeyman, iKeycmdnebo runmqakm.

Poznámka: Produkt IBM WebSphere 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 automatickým podpisem naleznete v tématu “Použití certifikátů s automatickým podpisem pro vzájemné ověření dvou správců front” na stránce 202.

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 WebSphere MQ podporuje tři různé typy CipherSpec. Podrobné informace naleznete v tématu “Interoperabilita Eliptické křivky a RSA CipherSpecs” na stránce 35 v tématu “Digitální certifikáty a kompatibilita CipherSpec v produktu IBM WebSphere MQ” na stránce 34 . 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 .

Použití správce klíčů iKeyman

Správce klíčů iKeyman neposkytuje metodu vyhovující standardu FIPS. Potřebujete-li spravovat certifikáty SSL nebo TLS způsobem, který je kompatibilní se standardem FIPS-, použijte příkaz **runmqakm** .

Chcete-li získat certifikát podepsaný držitelem pro vašeho správce front nebo klienta WebSphere MQ MQI, postupujte takto:

1. Spusťte grafické uživatelské rozhraní iKeyman 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 kterého chcete uložit certifikát, 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 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:
   - U správce front `ibmwebspheremq` následovaného názvem správce front přeloženého na malá písmena. Například pro `QM1`, `ibmwebspheremqqm1`, nebo,
   - U klienta WebSphere MQ `ibmwebspheremq` následovaného vaším přihlašovacím ID uživatele přeloženo na malá písmena, například `ibmwebspheremqmyuserid` .
10. Zadejte nebo vyberte hodnotu pro libovolné pole v poli **Distinguished name**nebo libovolné z polí **Subject alternative name** .
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.

z příkazového řádku,

Pomocí následujících příkazů vytvořte osobní certifikát podepsaný svým držitelem pomocí příkazu iKeycmd nebo runmqakm:

- Použití příkazu iKeycmd na systémech UNIX, Linux a Windows :

```
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_dsname` *`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
```

`-db` *`filename`*	Plně kvalifikovaný název souboru databáze klíčů CMS.
`-pw` *`password`*	Heslo pro databázi klíčů CMS.
`-label` *`label`*	Označení klíče připojené k certifikátu.
`-dn` *`distinguished_name`*	Rozlišovací název X.500 uzavřený ve dvojitých uvozovkách. Je povinný alespoň jeden atribut. Můžete zadat více atributů OU nebo DC.
`-size` *`key_size`*	Velikost klíče. Pro iKeycmdmůže být hodnota 512 nebo 1024. Pro runmqakm může být hodnota 512, 1024, 2048 nebo 4096.
`-x509version` *`version`*	Verze certifikátu X.509 , který má být vytvořen. Hodnota může být 1, 2 nebo 3. Výchozí hodnota je 3.
`-expire` *`days`*	Doba vypršení platnosti ve dnech certifikátu. Předvolba je 365 dní pro certifikát.

`-fips`	určuje, že příkaz má být spuštěn v režimu FIPS. Tento režim zakazuje použití kryptografické knihovny BSafe. Použije se pouze komponenta 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`	V případě runmqakm se používá algoritmus hašování použitý při vytváření certifikátu podepsaného držitelem. Tento hašovací algoritmus se používá k vytvoření podpisu přidruženého k nově vytvořenému certifikátu podepsaného (svým) držitelem. 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`.
`-sig_alg`	Pro iKeycmdse používá algoritmus asymetrického podpisu použitý pro vytvoření dvojice klíčů položky. Hodnota může být `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`, nebo `SHAWithRSA`. Výchozí hodnota je `SHA1WithRSA`.
`-san_dnsname` *`DNS_names`*	Čárka-nebo mezerami oddělený seznam názvů DNS pro vytvářený záznam.
`-san_emailaddr` *`email_addresses`*	Čárka nebo seznam e-mailových adres oddělených mezerou pro vytvářený záznam.
`-san_ipaddr` *`IP_addresses`*	Čárkami nebo mezerami oddělovaný seznam adres IP pro vytvářený záznam.

distributed *Požádání o osobní certifikát na systémech UNIX, Linux, and Windows*

Osobní certifikát můžete požádat pomocí produktu **strmqikm** (iKeyman) GUI, nebo z příkazového řádku pomocí příkazů **runmqckm** nebo **runmqakm** . 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 pomocí grafického uživatelského rozhraní iKeyman nebo z příkazového řádku, a to s následujícími aspekty:

- Produkt WebSphere 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 WebSphere MQ podporuje tři různé typy CipherSpec. Podrobné informace naleznete v tématu “Interoperabilita Eliptické křivky a RSA CipherSpecs” na stránce 35 v tématu “Digitální certifikáty a kompatibilita CipherSpec v produktu IBM WebSphere MQ” na stránce 34 .

- 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.
- Pouze příkaz runmqakm poskytuje volbu vyhovující FIPS.
- Používáte-li kryptografický hardware, přečtěte si téma "Požádání o osobní certifikát pro hardware PKCS #11" na stránce 137.

Použití uživatelského rozhraní iKeyman

Informace o této úloze

Správce klíčů iKeyman neposkytuje metodu vyhovující standardu FIPS. Potřebujete-li spravovat certifikáty SSL nebo 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 iKeyman 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 následující štítky:
   - Pro správce front zadejte hodnotu ibmwebspheremq a poté název správce front, který byl změněn na malá písmena. Příklad: Pro správce front s názvem QM1zadejte příkaz ibmwebspheremqqm1.
   - Pro IBM WebSphere MQ MQI clientzadejte ibmwebspheremq následovaný vaším přihlašovacím ID uživatele, vše, co je uvedeno malými; například ibmwebspheremqmyuserid .
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 122.
14. 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 -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.

-dn *rozlišující_název*
Určuje rozlišující název X.500 uzavřený ve dvojitých uvozovkách. Je povinný alespoň jeden atribut. Můžete zadat více atributů OU a DC.

-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. Tento režim zakazuje použití kryptografické knihovny BSafe. Použije se pouze komponenta ICC a tato komponenta musí být úspěšně inicializována 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. Hodnota může být 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, nebo 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.

Obnova existujícího osobního certifikátu na systémech UNIX, Linux, and Windows

Osobní certifikát můžete obnovit pomocí uživatelského rozhraní iKeyman , nebo pomocí příkazů **iKeycmd** nebo **runmqakm** .

Než začnete

Pokud máte požadavek používat větší velikosti klíčů pro vaše osobní certifikáty, kroky obnovy popsané níže nebudou fungovat, protože znovu vytvořený požadavek na certifikát je generován z existujícího klíče.

Postupujte podle kroků popsaných v části “Požádání o osobní certifikát na systémech UNIX, Linux, and Windows” na stránce 121 a vytvořte novou žádost o certifikát s použitím klíčových velikostí, které vyžadujete. Tento proces nahrazuje váš stávající klíč.

Informace o této úloze

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 iKeyman

Informace o této úloze

Správce klíčů iKeyman neposkytuje metodu vyhovující standardu FIPS. Potřebujete-li spravovat certifikáty SSL nebo 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 iKeyman pomocí příkazu **strmqikm** na systémech UNIX, 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 tlačítko **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 125.
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 **iKeycmd** nebo **runmqakm** , použijte následující příkazy:

- Použití produktu **iKeycmd** v systémech UNIX, Linux, and Windows :

```
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 systémech UNIX, Linux a Windows” na stránce 125.

Přijímání osobních certifikátů do úložiště klíčů v systémech UNIX, Linux a 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 správce klíčů iKeyman

Potřebujete-li provést správu certifikátů SSL v souladu se standardem FIPS, použijte příkaz runmqakm. Správce klíčů iKeyman neposkytuje metodu vyhovující standardu FIPS.

Ujistěte se, že soubor certifikátů, který má být importován, má oprávnění k zápisu pro aktuálního uživatele a poté následujícím postupem pro správce front nebo klienta WebSphere MQ MQI obdrží osobní certifikát do souboru databáze klíčů:

1. Spusťte grafické uživatelské rozhraní iKeyman pomocí příkazu **strmqikm** (na systému Windows UNIX and Linux).
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,

Pomocí následujících příkazů můžete přidat osobní certifikát do souboru databáze klíčů pomocí příkazu iKeycmd :

- V systému UNIX, Linux a Windowszadejte tento příkaz:

```
runmqckm -cert -receive -file filename -db filename -pw
password
        -format ascii
```

kde:

`-file filename`	je plně kvalifikovaný název souboru obsahujícího osobní certifikát.
`-db filename`	je plně kvalifikovaný název souboru databáze klíčů CMS.
`-pw password`	je heslo pro databázi klíčů CMS.
`-format ascii`	je formát certifikátu. Hodnota může být `ascii` pro Base64-encoded ASCII nebo `binary` pro binární data DER. Standardní hodnota je `ascii` .

Používáte-li kryptografický hardware, přečtěte si téma “Import osobního certifikátu do hardwaru vašeho PKCS #11” na stránce 139.

Extrakce certifikátu CA z úložiště klíčů

Chcete-li extrahovat certifikát CA, postupujte podle této procedury.

Použití správce klíčů iKeyman

Potřebujete-li provést správu certifikátů SSL v souladu se standardem FIPS, použijte příkaz runmqakm. Správce klíčů iKeyman neposkytuje metodu vyhovující standardu FIPS.

Na počítači, ze kterého chcete extrahovat certifikát CA, proveďte následující kroky:

1. Spusťte grafické uživatelské rozhraní iKeyman 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 iKeycmd :

- V systémech UNIX, Linux a Windows:

```
runmqckm -cert -extract -db filename -pw password -label label -target filename
         -format ascii
```

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`.

Extrahování veřejné části certifikátu podepsaného (svým) držitelem z úložiště klíčů v systémech UNIX, Linux a Windows

Uvedeným postupem extrahujte veřejnou část certifikátu podepsaného (svým) držitelem.

Použití správce klíčů iKeyman

Potřebujete-li provést správu certifikátů SSL v souladu se standardem FIPS, použijte příkaz runmqakm. Správce klíčů iKeyman neposkytuje metodu vyhovující standardu FIPS.

Na počítači, ze kterého chcete extrahovat veřejnou část certifikátu podepsaného sebou samým, proveďte následující kroky:

1. Spusťte grafické uživatelské rozhraní iKeyman pomocí příkazu **`strmqikm`** (na systémech UNIX, Linux a 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 extrahovat 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.
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 vlastním podpisem pomocí příkazu iKeycmd nebo runmqakm:

- V systémech UNIX, Linux a Windows:

```
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`.

Přidání certifikátu CA (nebo veřejné části certifikátu podepsaného sebou samým) do úložiště klíčů v systémech UNIX, 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: Je-li certifikát, který chcete přidat, v řetězu certifikátů, musíte přidat rovněž všechny certifikáty, které jsou v řetězu certifikátů nad tímto certifikátem. Musíte se ujistit, že certifikát je v kódování ASCII (UTF-8) nebo binárním kódování (DER), protože sada IBM Global Secure Toolkit (GSKit)

nepodporuje certifikáty s jinými typy kódování. Certifikáty musíte přidat v přísně sestupném pořadí počínaje kořenem a pokračujíce certifikátem CA, který v řetězu bezprostředně následuje pod ním.

Použití správce klíčů iKeyman

Potřebujete-li provést správu certifikátů SSL v souladu se standardem FIPS, použijte příkaz runmqakm. Správce klíčů iKeyman neposkytuje metodu vyhovující standardu FIPS.

Níže uvedené kroky proveďte na počítači, na který chcete přidat certifikát CA:

1. Spusťte grafické uživatelské rozhraní iKeyman pomocí příkazu **strmqikm** (na systémech UNIX, Linux a 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 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,

Při přidání certifikátu CA pomocí správce klíčů iKeycmd použijte tyto příkazy:

- V systému UNIX, Linux a Windowszadejte tento příkaz:

```
runmqckm -cert -add -db filename -pw password -label label -file filename
        -format ascii
```

kde:

`-db` *`filename`*	je název databáze klíčů CMS včetně cesty k souboru.
`-pw` *`password`*	je heslo pro databázi klíčů CMS.
`-label` *`label`*	je jmenovka přiložená k certifikátu.
`-file` *`filename`*	je název souboru obsahujícího certifikát.
`-format` *`ascii`*	je formát certifikátu. Hodnota může být `ascii` pro ASCII kódované formátem Base64 nebo `binary` pro binární data DER. Výchozí hodnota: `ascii`.

Export osobního certifikátu z úložiště klíčů

Chcete-li exportovat osobní certifikát, postupujte podle této procedury.

Použití správce klíčů iKeyman

Potřebujete-li provést správu certifikátů SSL v souladu se standardem FIPS, použijte příkaz runmqakm. Správce klíčů iKeyman neposkytuje metodu vyhovující standardu FIPS.

Na počítači, ze kterého chcete exportovat osobní certifikát, proveďte následující kroky:

1. Spusťte grafické uživatelské rozhraní iKeyman pomocí příkazu **strmqikm** (na systému Windows UNIX and Linux).
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,

Pomocí následujících příkazů exportujte osobní certifikát pomocí příkazu iKeycmd:

- V systémech UNIX, Linux a Windows:

```
runmqckm -cert -export -db filename -pw password -label label -type cms
        -target filename -target_pw password -target_type pkcs12
```

kde:

`-db` *filename*	je název databáze klíčů CMS včetně cesty k souboru.
`-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.

Import osobního certifikátu do úložiště klíčů v systémech UNIX, 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 sebou samým) do úložiště klíčů v systémech UNIX, Linux, and Windows” na stránce 128).

Soubory PKCS #12 by měly být považovány za dočasné a odstraněné po použití.

Použití správce klíčů iKeyman

Potřebujete-li spravovat certifikáty SSL způsobem, který vyhovuje standardu FIPS, použijte příkaz runmqakm. Správce klíčů iKeyman neposkytuje metodu vyhovující standardu FIPS.

Na počítači, na který chcete importovat osobní certifikát, proveďte následující kroky:

1. Spusťte grafické uživatelské rozhraní iKeyman 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. Toto okno umožňuje změnu jmenovek 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. Toto lze použít ke změně štítku osobního certifikátu na jmenovku vyžadovaného produktem WebSphere MQ za účelem přidružení certifikátu k určitému správci front nebo ke klientovi (například`ibmwebspheremqqm1`).
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 programu iKeycmd, použijte následující příkazy:

- V systémech UNIX, Linux a Windows:

```
runmqckm -cert -import -file filename -pw password -type pkcs12 -target filename
-target_pw password -target_type cms -label label
```

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 .

iKeycmd neposkytuje příkaz pro přímé změny návěští certifikátu. 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.

Import ze souboru Microsoft .pfx

Tuto proceduru použijte pro mport ze souboru Microsoft .pfx pomocí souboru iKeyman. Příkaz runmqakm nelze použít k importu souboru .pfx.

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 uživatelské rozhraní iKeyman pomocí příkazu **strmqikm** (v systémech Linux, UNIX nebo Windows). 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 ve tvaru `ibmwebspheremq`, za nímž následuje název správce front nebo přihlašovací ID uživatele klienta WebSphere MQ MQI uvedené malými písmeny.
21. Klepněte na tlačítko **OK**. Okno Změnit popisky je nyní odebráno a původní okno produktu IBM Key Management 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).

Návěští certifikátu není možné změnit pomocí iKeycmd

Import ze souboru PKCS #7

Nástroje iKeyman a iKeycmd nepodporují soubory PKCS #7 (.p7b). Použijte nástroj runmqckm k importu certifikátů ze souboru PKCS #7 .

Použijte následující příkaz k přidání certifikátu CA ze souboru PKCS #7 :

```
runmqckm -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 #7 PKCS.
`-label` *`label`*	je označení, které je přiřazeno certifikátu v cílové databázi. První certifikát bude mít zadaný popisek. Všechny ostatní certifikáty, jsou-li přítomny, jsou označeny štítkem s názvem subjektu.

Použijte následující příkaz k importu osobního certifikátu ze souboru PKCS #7 :

```
runmqckm -cert -import -db filename -pw password -type pkcs7 -target filename
-target_pw password -target_type cms -label label -new_label label
```

-db *filename*	je plně kvalifikovaný 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 cílové databáze klíčů.
-target_type *cms*	je typ databáze určený parametrem -target
-label *label*	je jmenovka certifikátu, který má být importován.
-new_label *label*	je popisek, který bude certifikát přiřazen v cílové databázi. Vynecháte-li volbu -new_label , použije se výchozí hodnota pro použití stejné jako volba -label .

Odstranění certifikátu z úložiště klíčů v systémech UNIX, Linux, and Windows

Tento postup slouží k odebrání osobních certifikátů nebo certifikátů CA.

Použití správce klíčů iKeyman

Potřebujete-li provést správu certifikátů SSL v souladu se standardem FIPS, použijte příkaz runmqakm. Správce klíčů iKeyman neposkytuje metodu vyhovující standardu FIPS.

1. Spusťte grafické uživatelské rozhraní iKeyman pomocí příkazu **strmqikm** (na systémech UNIX, Linux a 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 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 tlačítko **Exportovat/Importovat** a exportujte ji (viz “Export osobního certifikátu z úložiště klíčů” na stránce 129).
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,

Použijte následující příkazy k odstranění certifikátu pomocí iKeycmd nebo runmqakm:

- V systémech UNIX, Linux a Windows:

```
runmqckm -cert -delete -db filename -pw password -label label
```

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. Tento režim zakazuje použití kryptografické knihovny BSafe. Použije se pouze komponenta 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.

Generování silných hesel pro ochranu úložiště klíčů

Pomocí příkazu **runmqakm** můžete generovat silná hesla pro ochranu klíčů 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 UNIX 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 iKeyman není nutné, aby heslo ucitli nebo aby se z něj vytekla. Není to nutné, protože shell operačního systému nemá vliv na zadávání dat v těchto případech.

Konfigurace pro kryptografický hardware na systémech UNIX, Linux, and Windows

Šifrovací hardware pro správce front nebo klienta můžete nakonfigurovat mnoha způsoby.

Můžete nakonfigurovat kryptografický hardware pro správce front v systémech UNIX, Linux nebo Windows pomocí jedné z následujících metod:

- Použijte příkaz ALTER QMGR MQSC s parametrem SSLCRYP, jak je popsáno v tématu ALTER QMGR.
- Použijte IBM WebSphere MQ Explorer ke konfiguraci kryptografického hardwaru na systému UNIX, Linux nebo Windows . Další informace najdete v online nápovědě.

Šifrovací hardware pro klienta WebSphere MQ můžete nakonfigurovat na systémech UNIX, Linux nebo Okna 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_PCS11 , musí být popisek tokenu PKCS #11 určen zcela v menším případě.
- Nastavte pole **CryptoHardware** ve struktuře voleb konfigurace SSL, MQSCO, na volání MQCONNX. Další informace viz Přehled pro MQSCO.

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. To je popsáno v části “Správa certifikátů na hardwaru PKCS #11” na stránce 135.

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 WebSphere 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:
   - Na systémech UNIX, Linux, and Windows:

     ```
     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 produkt IBM WebSphere MQmusí být cms.)

   -stash
   Uloží heslo databáze klíčů do souboru.

   -fips
   Zakáže použití šifrovací knihovny BSafe. Použije se pouze komponenta ICC a tato komponenta musí být úspěšně inicializována 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 znakovém znakovém souboru ASCII v rozsahu 0x20 - 0x7E.

Volitelně můžete vytvořit databázi klíčů pomocí uživatelského rozhraní produktu **strmqikm** (iKeyman).

2. V systémech UNIX and Linux se přihlaste jako uživatel root. V systému Windows se přihlaste jako administrátor nebo jako člen skupiny MQM.
3. Spusťte uživatelské rozhraní iKeyman spuštěním příkazu **strmqikm** .
4. Klepněte na nabídku **Soubor databáze klíčů** > **Otevřít**.
5. Klepněte na volbu **Typ databáze klíčů** a vyberte volbu **PKCS11Direct**.
6. 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 iKeycmd a iKeyman jsou 64bitové programy. Externí moduly vyžadované podporou PKCS #11 se načtou do 64bitového procesu, a proto musíte mít pro administraci na šifrovacím hardwaru nainstalovanou 64bitovou knihovnu PKCS #11. 32bitové platformy Windows a Linux x86 jsou jedinými výjimkami, protože programy iKeyman a iKeycmd jsou na těchto platformách 32 bitové.

7. Do pole **Umístění** zadejte cestu:
   - V systémech UNIX 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.
8. Do pole **Heslo šifrovacího tokenu** zadejte heslo, které jste nastavili při konfiguraci kryptografického hardwaru.
9. 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 “13” na stránce 137.

   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**.
10. 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` .
11. V poli **Umístění** zadejte cestu, například:
    - Pro správce front: `/var/mqm/qmgrs/QM1/ssl`
    - Pro klienta IBM WebSphere MQ MQI: `/var/mqm/ssl`

    Klepněte na tlačítko **OK**. Otevře se okno Výzva k zadání hesla.
12. Zadejte heslo.

    Pokud jste v kroku “9” na stránce 137vybrali volbu **Otevřít existující databázový soubor sekundárního klíče** , zadejte do pole **Heslo** heslo.

    Pokud jste v kroku “9” na stránce 137vybrali 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 nescházíte, pokusy o spuštění kanálů SSL selžou, protože nemohou získat heslo požadované pro přístup k souboru databáze klíčů.

    c) Klepněte na tlačítko **OK**. Otevře se okno s potvrzením, že heslo je v souboru `key.sth` (pokud jste neuvedli jiný název kmene).
13. Klepněte na tlačítko **OK**. Zobrazí se rámec s informacemi o obsahu databáze klíčů.

Požádání o osobní certifikát pro hardware PKCS #11
Tento postup použijte buď pro správce front, nebo pro klienta IBM WebSphere MQ MQI, abyste požádali o osobní certifikát pro váš kryptografický hardware.

Použití uživatelského rozhraní iKeyman

Informace o této úloze

Poznámka: Produkt WebSphere 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 iKeyman , postupujte takto:

1. Postupujte takto, abyste mohli pracovat s vaším kryptografickým hardwarem. Viz “Správa certifikátů na hardwaru PKCS #11” na stránce 135.
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 následující štítky:
   - Pro správce front zadejte hodnotu `ibmwebspheremq` a poté název správce front, který byl změněn na malá písmena. Příklad: Pro správce front s názvem `QM1`zadejte příkaz `ibmwebspheremqqm1`.
   - Do pole IBM WebSphere MQ MQI clientzadejte řetězec `ibmwebspheremq` následovaný vaším přihlašovacím ID uživatele, vše malými písmeny; například `ibmwebspheremqmyuserid` .
4. 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.
5. Do pole **Zadejte název souboru, do kterého chcete uložit žádost o certifikát** , buď přijměte výchozí `certreq.arm`, nebo zadejte novou hodnotu s úplnou cestou.
6. Klepněte na tlačítko **OK**.

   Otevře se okno Potvrzení.
7. 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 “5” na stránce 138.
8. 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 -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.

-dn *rozlišující_název*
Určuje rozlišující název X.500 uzavřený ve dvojitých uvozovkách. Je povinný alespoň jeden atribut. Můžete zadat více atributů OU a DC.

-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. Tento režim zakazuje použití kryptografické knihovny BSafe. Použije se pouze komponenta ICC a tato komponenta musí být úspěšně inicializována 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. Hodnota může být 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, nebo 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.

Import osobního certifikátu do hardwaru vašeho PKCS #11
Tento postup použijte buď pro správce front, nebo pro klienta IBM WebSphere MQ MQI pro import osobního certifikátu do vašeho kryptografického hardwaru.

Použití správce klíčů iKeyman

Postup

Chcete-li požádat o osobní certifikát z uživatelského rozhraní iKeyman , postupujte takto:

1. Postupujte takto, abyste mohli pracovat s vaším kryptografickým hardwarem. Viz “Správa certifikátů na hardwaru PKCS #11” na stránce 135.
2. Klepněte na tlačítko **Přijmout**. Otevře se okno Přijmout certifikát ze souboru.
3. Vyberte volbu **Datový typ** nového osobního certifikátu; například `Base64-encoded ASCII data` pro soubor s příponou `.arm` .
4. Zadejte název souboru certifikátu a umístění pro nový osobní certifikát, nebo klepněte na tlačítko **Procházet** a vyberte název a umístění.
5. 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.
6. Klepněte na tlačítko **Ano** nebo **Ne**. Otevře se okno Zadat jmenovku.
7. Zadejte popisek.

   Stejný popisek můžete použít například při požadavku na osobní certifikát. Všimněte si, že štítek musí být ve správném formátu IBM WebSphere MQ :

   - Pro správce front `ibmwebspheremq` následovaný názvem správce front malými písmeny. Například pro správce front s názvem QM1bude jmenovka následující: `ibmwebspheremqqm1`.
   - V případě klienta IBM WebSphere MQ MQI `ibmwebspheremq` následovaného přihlašovacím ID uživatele malými písmeny. Například pro ID uživatele `MyUserID`bude jmenovka následující: `ibmwebspheremqmyuserid`.
8. 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.

z příkazového řádku,

Postup

Chcete-li požádat o osobní certifikát z příkazového řádku, proveďte následující kroky:

1. Otevřete příkazové okno, které je nakonfigurované pro vaše prostředí.
2. Zadejte příslušný příkaz pro váš operační systém a konfiguraci:

   - Na systémech Windows, UNIX and Linux použijte jeden z následujících příkazů:

     ```
     runmqckm -cert -receive -file filename -crypto path
     -tokenlabel hardware_token -pw hardware_password -format cert_format
     ```

     ```
     runmqakm -cert -receive -file filename -crypto path
     -tokenlabel hardware_token -pw hardware_password -format cert_format -fips
     ```

   kde:

   -file *název_souboru*
   Uvádí plně kvalifikovaný název souboru, který obsahuje osobní certifikát.

   -crypto *cesta*
   Uvádí úplnou cestu ke knihovně PKCS #11 dodané s hardwarem.

   -tokenlabel *hardwareční_token*
   Uvádí jmenovku poskytnutou části úložiště kryptografického hardwaru během instalace.

   -pw *heslo_hardwaru_hardwaru*
   Uvádí heslo pro přístup k 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 je spuštěn v režimu FIPS Tento režim zakazuje použití šifrovací knihovny BSafe. Použije se pouze komponenta ICC a tato komponenta musí být úspěšně inicializována 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.

Identifikace a ověřování uživatelů

Uživatele můžete identifikovat a ověřovat pomocí struktury MQCSP nebo několika typů uživatelského ukončovacího programu.

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.

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 jedná o uživatele klientské aplikace WebSphere MQ . V této situaci dochází ke vzájemnému ověřování mezi dvěma správci front nebo mezi správcem front a uživatelem klientské aplikace WebSphere MQ MQI.

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” na stránce 100.

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.

SSL (Secure Sockets Layer) a TLS (Transport Layer Security) používají techniky PKI jako ty, které právě popisují. Další informace o tom, jak SSL a TLS provést ověření, viz “Koncepce zabezpečení SSL (Secure Sockets Layer) a TLS (Transport Layer Security)” 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 220. 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 73.

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 naleznete v části “Mapování identity ve výstupu rozhraní API a ukončení přeletu rozhraní API” na stránce 145.

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.

Oprávnění uživatelé

Privilegovaný uživatel je takový, který má úplná administrativní oprávnění pro produkt WebSphere MQ.

Kromě uživatelů uvedených v následující tabulce jsou členy libovolné skupiny s oprávněním `+crt` pro fronty nepřímo administrátory. Podobně platí, že každý uživatel, který má oprávnění `+set` na správci front, a oprávnění `+put` ve frontě příkazů je administrátor.

Tato oprávnění byste neměli udělovat běžným uživatelům a aplikacím.

Tabulka 13. Oprávnění uživatelé podle platformy.

Tabulka privilegovaných uživatelů. Na systémech Windows, SYSTEM, všichni členové skupiny mqm a všichni členové skupiny Administrátoři jsou privilegovaní uživatelé. V systémech UNIX and Linux jsou všichni členové skupiny mqm privilegovaní uživatelé. V systému IBM ijsou všichni členové skupiny qmqmadm (uživatelé) qmqm a qmqmadm, všichni členové skupiny qmqmadm a všichni uživatelé definovaní s nastavením *ALLOBJ, privilegovaní uživatelé.

Platforma	**Oprávnění uživatelé**
Systémy Windows	• SYSTÉM • Členové skupiny mqm • Členové skupiny administrátorů
Systémy UNIX and Linux	• Členové skupiny mqm

Identifikace a ověřování uživatelů pomocí struktury MQCSP

Strukturu parametrů zabezpečení připojení MQCSP můžete zadat na volání MQCONNX.

Struktura parametrů zabezpečení připojení MQCSP obsahuje ID uživatele a heslo, které může služba autorizace použít k identifikaci a ověření uživatele.

Komponenta autorizační služba dodaná s produktem IBM WebSphere MQ se nazývá OAM (Object Authority Manager). OAM autorizuje uživatele na základě ID obsaženého ve struktuře MQCSP, ale neověřuje heslo. Je možné implementovat ověření platnosti hesla v autorizační službě pomocí zřetězených uživatelských procedur s OAM, nebo nahrazením OAM alternativní autorizační službou.

V uživatelské proceduře zabezpečení můžete změnit MQCSP.

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 straně klienta kanálu MQI se agent MCA obvykle chová jménem uživatele klientské aplikace WebSphere MQ MQI. V této situaci dochází ke vzájemnému ověřování mezi dvěma správci front nebo mezi správcem front a uživatelem klientské aplikace WebSphere MQ MQI.

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” na stránce 100.

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.

SSL (Secure Sockets Layer) a TLS (Transport Layer Security) používají techniky PKI jako ty, které právě popisují. Další informace o tom, jak SSL provádí ověření, viz “Koncepce zabezpečení SSL (Secure Sockets Layer) a TLS (Transport Layer Security)” 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 220. 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 73.

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 145.

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 navázání komunikace přes zabezpečení SSL se komunikující partneři navzájem ověřují 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).

V systémech UNIX, Linux a Windows podpora zabezpečení SSL produktu WebSphere MQ kontroluje odvolané certifikáty pomocí protokolu OCSP (Online Certificate Status Protocol) nebo pomocí seznamů CRL a ARL na serverech LDAP (Lightweight Directory Access Protocol). Preferovaná metoda je OCSP. Třídy IBM WebSphere MQ classes for Java a IBM WebSphere MQ classes for JMS nemohou používat informace OCSP v souboru s tabulkou definic kanálů klienta. Nicméně můžete OCSP nakonfigurovat podle popisu uvedeného v kapitole Používání protokolu certifikátů online.

V produktech z/Os a produktu IBM i WebSphere MQ SSL kontroluje odvolané certifikáty pomocí seznamů CRL a ARL pouze na serverech LDAP.

Další informace o certifikátu

Oprávnění, viz “digitální certifikáty” na stránce 9.

Zrušené certifikáty and OCSP

Produkt IBM WebSphere 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 se týkají pouze produktu WebSphere MQ v systémech Windows a UNIX and Linux.

Při kontrole stavu odvolání digitálního certifikátu pomocí protokolu OCSP produkt WebSphere 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 nebo SSL 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 WebSphere MQ nezískal přístup k odpovídacímu modulu OCSP.
- Odpovídací modul OCSP odeslal odezvu, ale produktu WebSphere 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 WebSphere MQ výsledek protokolu OCSP `Neznámý`, jeho chování bude záviset na nastavení atributu OCSPAuthentication. Pro správce front je tento atribut umístěn v sekci SSL souboru `qm.ini` (v systémech UNIX and Linux) nebo v registru systému Windows. Lze ji nastavit pomocí Průzkumníka IBM WebSphere MQ . U klientů je umístěn v sekci SSL konfiguračního souboru klienta.

Je-li přijat výsledek `Neznámý` a atribut OCSPAuthentication je nastaven na hodnotu REQUIRED (výchozí hodnota), produkt WebSphere 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 WebSphere 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 WebSphere 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 takovém případě nepotřebujete nastavovat žádný další certifikát. Kroky, které jste již provedli při vytváření spojení SSL, postačují 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. Jelikož je odezva OCSP odesílána společně s certifikátem použitým k jejímu podepsání (a tento certifikát je podepsán CA, která je již pro účel propojení SSL považována za důvěryhodnou), není třeba provádět žádné další nastavování certifikátů.
- 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 sebou samým) do úložiště klíčů v systémech UNIX, Linux, and Windows” na stránce 128. Přidávaný certifikát CA je standardně přidán jako důvěryhodný kořenový certifikát, což je v tomto kontextu povinné nastavení. Není-li tento certifikát přidán, produkt WebSphere MQ nemůže ověřit digitální podpis v odezvě OCSP a kontrola OCSP vrátí výsledek Neznámý, následkem čehož může produkt IBM WebSphere MQ zavřít kanál, vyžaduje-li to nastavení atributu OCSPAuthentication.

Protokol OCSP (Online Certificate Status Protocol) v aplikacích klienta Java a JMS

Kvůli omezení rozhraní JAVA API může produkt WebSphere MQ používat kontrolu odvolání certifikátů OCSP (Online Certificate Status Protocol) pro zabezpečené sokety SSL a TLS pouze tehdy, je-li protokol OCSP povolen pro celý proces virtuálního stroje Java (JVM). 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 rozhraní API java.security.Security.setProperty(), jež podléhá veškerým platným zásadám modulu 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.

Název vlastnosti	Popis
ocsp.responderURL	Tato vlastnost nese hodnotu, jež odpovídá adrese URL, která určuje umístění odpovídacího modulu OCSP. Příklad: `ocsp.responderURL=http://ocsp.example.net:80`. Při výchozím nastavení se umístění odpovídacího modulu OCSP určuje implicitně z ověřovaného certifikátu. Vlastnost se používá, pokud v certifikátu chybí rozšíření Authority Information Access (definované v dokumentu RFC 3280) nebo pokud vyžaduje potlačení.
ocsp.responderCertSubjectName	Tato vlastnost nese hodnotu, jež určuje název subjektu certifikátu odpovídacího modulu OCSP. Příklad: `ocsp.responderCertSubjectName="CN=OCSP Responder, O=XYZ Corp"`. Při výchozím nastavení certifikát odpovídacího modulu OCSP má vydavatele, který vydal ověřovaný certifikát. Tato vlastnost identifikuje certifikát odpovídacího modulu OCSP v případě, že nelze použít výchozí hodnotu. Jeho hodnota je řetězec úplného názvu (definovaný RFC 2253), který identifikuje certifikát v sadě certifikátů poskytnutých během ověřování cest certifikátu. V případech, kdy samotný název subjektu nepostačuje k jedinečné identifikaci certifikátu, musejí být místo něj použity obě tyto vlastnosti: ocsp.responderCertIssuerName a ocsp.responderCertSerialNumber. Je-li tato vlastnost nastavena, budou vlastnosti ocsp.responderCertIssuerName a ocsp.responderCertSerialNumber ignorovány.
ocsp.responderCertIssuerName	Tato vlastnost nese hodnotu odpovídající názvu vydavatele certifikátu odpovídacího modulu OCSP. Příklad: `ocsp.responderCertIssuerName="CN=Enterprise CA, O=XYZ Corp"`. Při výchozím nastavení certifikát odpovídacího modulu OCSP má vydavatele, který vydal ověřovaný certifikát. Tato vlastnost identifikuje certifikát odpovídacího modulu OCSP v případě, že nelze použít výchozí hodnotu. Jeho hodnota je řetězec úplného názvu (definovaný RFC 2253), který identifikuje certifikát v sadě certifikátů poskytnutých během ověřování cest certifikátu. Je-li tato vlastnost nastavena, musí být nastavena rovněž vlastnost ocsp.responderCertSerialNumber. Tato vlastnost je ignorována, je-li nastavena vlastnost ocsp.responderCertSubjectName.
ocsp.responderCertSerialNumber	Tato vlastnost nese hodnotu, jež je sériovým číslem certifikátu odpovídacího modulu OCSP. Příklad: `ocsp.responderCertSerialNumber=2A:FF:00`. Při výchozím nastavení certifikát odpovídacího modulu OCSP má vydavatele, který vydal ověřovaný certifikát. Tato vlastnost identifikuje certifikát odpovídacího modulu OCSP v případě, že nelze použít výchozí hodnotu. Tato hodnota je řetězec hexadecimálních číslic (jako oddělovače mohou být použity dvojtečka a mezera) identifikující certifikát v sadě certifikátů poskytnutých během ověřování cest certifikátu. Je-li tato vlastnost nastavena, musí být nastavena rovněž vlastnost ocsp.responderCertIssuerName. Tato vlastnost je ignorována, je-li nastavena vlastnost ocsp.responderCertSubjectName.

Dříve než povolíte OCSP tímto způsobem, zvažte tyto aspekty:

- Nastavení konfigurace OCSP ovlivňují všechny zabezpečené sokety v procesu JVM. V některých případech může mít tato konfigurace nežádoucí důsledky, je-li prostředí JVM sdíleno s kódem jiné aplikace, jež používá zabezpečené sokety SSL nebo TLS. Zajistěte, aby zvolená konfigurace OCSP byla vhodná pro všechny aplikace, jež běží ve stejném prostředí JVM.

- Při použití opravy pro vaše prostředí JRE může dojít k přepsání souboru java.security. Při použití prozatímních oprav a balíčků údržby produktu zabraňte přepsání souboru java.security. Po použití balíčku údržby může být nezbytné znovu provést vlastní změny v souboru java.security. Z tohoto důvodu může být výhodnější provést nastavení konfigurace OCSP prostřednictvím rozhraní API java.security.Security.setProperty().
- Povolení kontroly OCSP se projeví pouze v případě, že je povolena rovněž kontrola odvolání. Kontrola odvolání se povoluje metodou `PKIXParameters.setRevocationEnabled()`.
- Používáte-li zachytávač AMS Java Interceptor, který je popsán v tématu Povolení kontroly OCSP v nativních zachytávačích, vyhněte se použití konfigurace OCSP java.security,která by kolidovala s konfigurací AMS OCSP v konfiguračním souboru úložiště klíčů.

Práce se seznamy odvolaných certifikátů a seznamy odvolaných autorit

Podpora produktu WebSphere MQpro seznamy CRL a ARL se liší podle platformy.

Podpora CRL a ARL na každé platformě je následující:

- V systému z/OSSSL System 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 WebSphere MQ udržuje mezipaměť seznamů CRL a ARL, k nimž bylo přistupována během předchozích 12 hodin.

Když správce front nebo klient WebSphere MQ MQI obdrží certifikát, zkontroluje seznam CRL a potvrdí, že je certifikát stále platný. WebSphere MQ first checks in the cache, if there is a cache. Pokud seznam CRL není v mezipaměti, produkt WebSphere MQ dotazuje umístění serverů LDAP CRL v pořadí, v jakém se vyskytují v seznamu názvů objektů ověřovacích informací určených atributem *SSLCRLNamelist* , dokud produkt WebSphere MQ nenajde dostupný seznam CRL. Není-li seznam názvů zadán nebo je-li zadán s prázdnou hodnotou, seznamy odvolaných certifikátů se nekontrolují.

Další informace o protokolu LDAP naleznete v tématu Použití služeb protokolu LDAP (Lightweight Directory Access Protocol) s produktem WebSphere MQ for Windows.

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 WebSphere MQ SSL 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 12 na stránce 151 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 IBM.

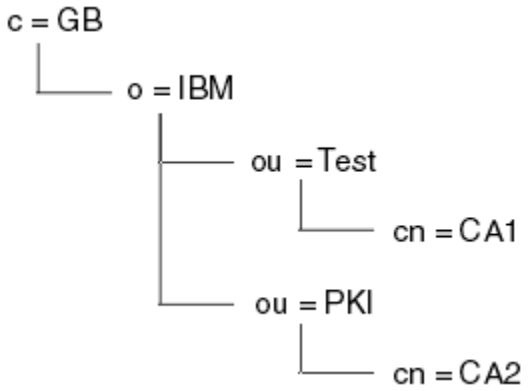
```
dn: o=IBM, c=GB
o: IBM
objectclass: top
objectclass: organization

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 12. Ukázkový soubor LDIF pro certifikační autoritu. To se může lišit od implementace k implementaci.

Obrázek 13 na stránce 151 ukazuje strukturu DIT, kterou váš server LDAP vytváří při načtení ukázkového souboru LDIF zobrazeného v produktu Obrázek 12 na stránce 151 společně s podobným souborem pro CA2, imaginárním certifikačním úřadem, který je zřízen organizací PKI, také v rámci IBM.



Obrázek 13. Příklad struktury informačního stromu adresáře LDAP

Produkt WebSphere 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 WebSphere 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 151.

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.

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 *SSLCRLNamelist* .

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.

   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.

   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.
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 *SSLCRLNamelist*. Počáteční hodnota správce front pro tento atribut je prázdná.

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.

Přístup k seznačkám CRL a ARL pomocí produktu IBM WebSphere MQ Explorer

Produkt IBM WebSphere MQ Explorer můžete použít k tomu, abyste správci front sděli, jak přistupovat k seznamu 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 **Namelists** 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 152) 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. Do pole **Seznam názvů CRL** zadejte název seznamu názvů (z kroku “3.a” na stránce 153).

Přístup k seznačkám CRL a ARL s klientem IBM WebSphere MQ MQI

K dispozici jsou tři možnosti určení serverů LDAP, které obsahují seznamy odvolaných certifikátů pro kontrolu klienta IBM WebSphere MQ MQI.

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 klienta WebSphere MQ MQI spuštěného na systému Linux (platforma zSeries).

Umístění odpovídacího modulu OCSP a serverů LDAP, které obsahují seznamy odvolaných certifikátů (CRL)
Na klientském systému IBM WebSphere MQ MQI můžete určit umístění odpovídacího modulu OCSP a serverů LDAP (Lightweight Directory Access Protocol), které uchovávají seznamy zrušených certifikátů (CRL).

Tato umístění můžete určit třemi způsoby, zde jsou uvedeny v pořadí klesající priority.

Při problémech aplikace klienta WebSphere MQ MQI se zobrazí 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 klient WebSphere MQ MQI vyžaduje pro přístup k odpovídacímu modulu OCSP nebo k serveru LDAP, který obsahuje seznamy odvolaných certifikátů (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 klient WebSphere MQ MQI 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.

Objekt ověřovacích informací s typem AUTHTYPE (OCSP) se nepoužívá pro použití ve správcích front systému 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 povolit klientovi WebSphere MQ MQI přístup k odpovídacímu modulu OCSP nebo serverům LDAP, které obsahují seznamy odvolaných certifikátů, mohou být atributy jednoho nebo více objektů ověřovacích informací zahrnuty do tabulky definic kanálů klienta. Takové atributy můžete zahrnout do jednoho z následujících způsobů:

Na platformách serveru AIX, HP-UX, Linux, Solaris a Windows

Můžete definovat seznam názvů, který obsahuje názvy jednoho nebo více objektů ověřovacích informací. Poté můžete nastavit atribut správce front **SSLCRLNameList**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, je-li vyžadován, klient WebSphere MQ MQI se může 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 **SSLCRLNameList**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 klient WebSphere MQ MQI v daném systému používat umístění odvolaných certifikátů v tabulce CCDT pro přístup k odpovídacímu modulu OCSP nebo serverům LDAP, které obsahují seznamy odvolaných certifikátů 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 **SSLCRLNameList**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.

Použití Active Directory v systému 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 třídami IBM WebSphere MQ pro třídy Java a IBM WebSphere MQ pro platformu JMS

Třídy IBM WebSphere MQ pro třídy Java a IBM WebSphere MQ pro přístup k seznami přístupových práv platformy JMS se liší od jiných platforem.

Informace o práci s seznamy CRL a ARL s třídami IBM WebSphere MQ for Java naleznete v tématu Použití seznamů odvolaných certifikátů.

Informace o práci s seznamy CRL a ARL s třídami IBM WebSphere MQ pro platformu JMS naleznete v tématu Vlastnost objektu SSLCERTSTORES.

Manipulace s objekty ověřovacích informací

Objekty ověřovacích informací můžete manipulovat pomocí příkazů MQSC nebo PCF, nebo můžete pracovat s produktem IBM WebSphere 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 skriptu (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 také použít Průzkumníka produktu WebSphere MQ .

Autorizace přístupu k objektům

Tento oddíl obsahuje informace o používání správce oprávnění k objektu a ukončovacích programů kanálu k řízení přístupu k objektům.

V systémech UNIX, 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. Obsahuje také kontrolní seznam, který můžete použít k určení úloh, které mají být použity při zabezpečení systému, a pokyny pro udělení oprávnění uživatelům k administraci produktu IBM WebSphere MQ a k práci s objekty produktu IBM WebSphere MQ . Pokud dodané bezpečnostní mechanismy nevyhovují vašim potřebám, můžete vyvinout vlastní uživatelské programy kanálu.

Řízení přístupu k objektům pomocí OAM v systémech UNIX, Linux a Windows

Správce oprávnění k objektu (OAM) poskytuje rozhraní příkazového řádku pro udělování a odebírání oprávnění k objektům produktu WebSphere MQ .

Musíte být vhodně autorizováni pro použití těchto příkazů, jak je popsáno v “Oprávnění k administraci produktu IBM WebSphere MQ v systémech UNIX, Linux, and Windows” na stránce 192. ID uživatele, která jsou autorizována pro administraci produktu WebSphere MQ , mají oprávnění *superuživatele* ke správci front, což znamená, že jim nemusíte udělit další oprávnění k vydávání jakýchkoli požadavků nebo příkazů MQI.

Udělení přístupu k objektu IBM WebSphere MQ v systémech UNIX, Linux, and Windows

Pomocí řídicího příkazu **setmqaut** nebo příkazu PCF **MQCMD_SET_AUTH_REC** poskytněte uživatelům a skupinám uživatelů přístup k objektům produktu IBM WebSphere MQ .

Úplnou definici řídicího příkazu **setmqaut** a jeho syntaxi naleznete v souboru setmqauta v úplné definici příkazu **MQCMD_SET_AUTH_REC** PCF a jeho syntaxi viz Nastavit záznam 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*; toto 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 systémech UNIX, Linux, and Windows” na stránce 157.
- 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. Na systémech 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 použití příkazu `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. Na systémech UNIX 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 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.

Použití generických profilů OAM na systémech UNIX, Linux, and Windows

Generické profily OAM vám umožňují nastavit oprávnění, které má uživatel k mnoha objektům najednou, spíše než abyste museli vydat samostatné příkazy **setmqaut** pro každý jednotlivý objekt, když je vytvářen.

Použití generických profilů v příkazu **setmqaut** umožňuje nastavit generické oprávnění pro všechny objekty, které vyhovují tomuto profilu.

Tato kolekce témat popisuje použití generických profilů podrobněji.

Použití zástupných znaků v profilech OAM

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. Například, v `ABC.DEF.GHI`jsou kvalifikátory `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: Používáte-li na systémech UNIX and Linux zástupné znaky, **musíte** uzavřít název profilu do jednoduchých uvozovek.

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:

```
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, ve výše uvedeném příkladu, fronta AB.CD má autoritu **get** (AB.C* je více specifická než AB. *).

Porovnáváte-li generické znaky, pořadí *specifičnosti* je:

1. ?
2. *
3. **

Probíhá výpis nastavení profilu

Úplnou definici řídicího příkazu **dmpmqaut** a jeho syntaxi naleznete v části dmpmqauta v úplné definici příkazu **MQCMD_INQUIRE_AUTH_RECS** PCF a jeho 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 přibližně takto:

   ```
   profile:     a.b.*
   object type: queue
   entity:      user1
   type:        principal
   authority:   get, browse, put, inq
   ```

   Poznámka: Ačkoli uživatelé produktu UNIX 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 bude vypadat 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. *, fronty typu.

```
dmpmqaut -m qmgr1 -n a.b.* -t q
```

Výsledný výpis bude vypadat 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 bude vypadat 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 bude vypadat přibližně takto:

```
profile: q1, type: queue
profile: q*, type: queue
profile: name.*, type: namelist
profile: pr1, type: process
```

Poznámka: Pro produkt WebSphere MQ pouze pro systém 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
```

Použití zástupných znaků v profilech OAM

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.BEFatd`.

Dostupné zástupné znaky jsou:

?

Otazník (?) zastupuje libovolný jeden znak. Například `AB.?D` se vztahuje 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` se vztahuje na objekty `ABC.DEF.JKLa 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.JKLa 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: Používáte-li na systémech UNIX and Linux zástupné znaky, **musíte** uzavřít název profilu do jednoduchých uvozovek.

Priority profilu

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, ve výše uvedeném příkladu, fronta AB.CD má autoritu **get** (AB.C* je více specifická než AB. *).

Porovnáváte-li generické znaky, pořadí *specifičnosti* je:

1. ?
2. *
3. **

Probíhá výpis nastavení profilu

Chcete-li vypsat aktuální autorizace přidružené k určenému profilu, použijte řídicí příkaz **dmpmqaut** nebo příkaz **MQCMD_INQUIRE_AUTH_RECS** PCF.

Úplnou definici řídicího příkazu **dmpmqaut** a jeho syntaxi naleznete v části dmpmqauta v úplné definici příkazu **MQCMD_INQUIRE_AUTH_RECS** PCF a jeho 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 UNIX 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: Pro produkt WebSphere MQ pouze pro systém 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
```

Zobrazení nastavení přístupu

Použijte řídicí příkaz **dspmqaut** nebo příkaz **MQCMD_INQUIRE_ENTITY_AUTH** PCF pro zobrazení autorizací, které určitá činitel nebo skupina má pro konkrétní objekt.

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 části dmpmqauta v úplné definici příkazu **MQCMD_INQUIRE_ENTITY_AUTH** PCF a její syntaxe viz Inquire Entity Authority.

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
```

Změna a zrušení přístupu k objektu IBM WebSphere MQ

Chcete-li změnit úroveň přístupu, kterou má uživatel nebo skupina k objektu, použijte příkaz **setmqaut** . Chcete-li zrušit přístup konkrétního uživatele, který je členem skupiny, která má oprávnění, odeberte uživatele ze skupiny.

Proces odebrání uživatele ze skupiny je popsán v:

- “Vytvoření a správa skupin v systému Windows” na stránce 80
- “Vytvoření a správa skupin v systému HP-UX” na stránce 82
- “Vytvoření a správa skupin v systému AIX” na stránce 83
- “Vytvoření a správa skupin v systému Solaris” na stránce 84
- “Vytvoření a správa skupin v systému Linux” na stránce 85

.

ID uživatele, který vytvoří objekt IBM WebSphere 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 souboru setmqauta v úplné definici příkazu **MQCMD_INQUIRE_ENTITY_AUTH** PCF a jeho syntaxi naleznete v tématu Inquire Entity Authority.

V systému Windowsodstraňte položky OAM odpovídající konkrétnímu uživatelskému účtu systému Windows před odstraněním profilu uživatele. Je nemožné odstranit záznamy OAM po odstranění uživatelského účtu.

Prevence kontrol přístupu k zabezpečení v systémech UNIX, Linux, and Windows

Chcete-li vypnout všechny kontroly zabezpečení, můžete zakázat funkci OAM. To může být vhodné pro testovací prostředí. Pokud jste zakázali nebo odebrali jste OAM, nemůžete přidat 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 (pokud tuto akci provedete později, nemůžete později přidat produkt OAM):

  See Proměnné prostředí for more information about the implications of setting the MQSNOAUT variable.
- Upravte konfigurační soubor správce front a odeberte službu. (Pokud tak učiníte, nemůžete později přidat OAM.)

Pokud používáte setmqaut nebo dspmqaut, zatímco OAM je zablokovaný, všimněte si následujících bodů:

- OAM neověřuje zadaného činitele nebo skupinu, což znamená, že příkaz může přijmout neplatné hodnoty .
- OAM neprovádí bezpečnostní kontroly a označuje, že všichni činitelé a skupiny jsou autorizováni provádět všechny použitelné operace s objekty.

Upozornění: Je-li objekt OAM odebrán, nelze jej vrátit zpět do existujícího správce front. Tento je tím, že parametr OAM musí být na místě vytvoření objektu. Chcete-li znovu použít produkt WebSphere MQ OAM poté, co byl odebrán, musí být správce front znovu sestaven.

Související pojmy

Instalovatelné služby

Udělení požadovaného přístupu k prostředkům

Prostřednictvím tohoto tématu můžete určit, které úlohy mají být provedeny při použití zabezpečení v systému WebSphere MQ .

Informace o této úloze

Během této úlohy rozhodujete o tom, jaké akce jsou nezbytné pro použití odpovídající úrovně zabezpečení na prvky instalace produktu WebSphere 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 164.
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 169.
4. Mají tito uživatelé přístup jen pro čtení ke všem prostředkům správce front?
   a) Ne: Přejděte na další otázku.
   b) Ano: Viz “Udělení přístupu pouze pro čtení ke všem prostředkům ve správci front” na stránce 174.
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 175.
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 176
   b) Ano: Viz “Povolení připojení uživatelských aplikací k vašemu správci front” na stránce 177.

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 14. 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 165 .

Tabulka 14. Udělení částečného administrativního přístupu k podmnožině prostředků správce front (pokračování)	
Uživatelé potřebují spravovat objekty tohoto typu	**Provést tuto akci**
Témata	Udělte částečný administrativní přístup k požadovaným tématům, jak je popsáno v tématu “Udělení omezeného administrativního přístupu k některým tématům” na stránce 166 .
Kanály	Udělte částečný administrativní přístup k požadovaným kanálům, jak je popsáno v tématu “Udělení omezeného administrativního přístupu k některým kanálům” na stránce 166
Správce front	Udělte částečný administrativní přístup ke správci front, jak je popsáno v tématu “Udělení omezeného administrativního přístupu ke správci front” na stránce 167 .
Procesy	Udělte částečný administrativní přístup k požadovaným procesům, jak je popsáno v tématu “Udělení omezeného administrativního přístupu k některým procesům” na stránce 168 .
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 168
Služby	Udělte částečný administrativní přístup k požadovaným službám, jak je popsáno v tématu “Udělení omezeného administrativního přístupu k některým službám” na stránce 169

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.

Procedura

- Pro systémy UNIX, Linux a Windows zadejte tento příkaz:

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName ReqdAction
```

- Názvy proměnných mají následující význam:

  QMgrName
  Název správce front. V systému z/OSmůže tato hodnota představovat také název 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:

– V systémech UNIX, Linux a Windows se všechny kombinace následujících autorizací: + chg, + clr, + dlt, + dsp. Oprávnění + alladm je ekvivalentní s + chg + clr + dlt + dsp.

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.

Procedura

- Pro systémy UNIX, Linux a Windows zadejte tento příkaz:

```
setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName ReqdAction
```

- 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:

– V systémech UNIX, Linux a Windows se všechny kombinace následujících autorizací: + chg, + clr, + crt, + dlt, + dsp. + CTRL. Oprávnění + alladm je ekvivalentní s + chg + clr + dlt + dsp.

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.

Procedura

- Pro systémy UNIX, Linux a Windows zadejte tento příkaz:

```
setmqaut -m QMgrName -n ObjectProfile -t channel -g GroupName ReqdAction
```

- Názvy proměnných mají následující význam:

QMgrName
Název správce front. V systému z/OSmůže tato hodnota představovat také název 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:

– V systémech UNIX, Linux a Windows se všechny kombinace následujících autorizací: + chg, + clr, + crt, + dlt, + dsp. + ctrl, + ctrlx. Oprávnění + alladm je ekvivalentní s + chg + clr + dlt + dsp.

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.

Procedura

- Pro systémy UNIX, Linux a Windows zadejte tento příkaz:

```
setmqaut -m QMgrName -n ObjectProfile -t qmgr -g GroupName ReqdAction
```

- Pro IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*MQM) USER(GroupName) AUT(ReqdAction)
MQMNAME('QMgrName')
```

Výsledky

Chcete-li určit příkazy MQSC, které může uživatel provádět s tímto správcem 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:

- V systémech UNIX, Linux a Windows se 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.

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.

Procedura

- Pro systémy UNIX, Linux a Windows zadejte tento příkaz:

```
setmqaut -m QMgrName -n ObjectProfile -t process -g GroupName ReqdAction
```

- 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:

  – V systémech UNIX, Linux a Windows se všechny kombinace následujících autorizací: + chg, + clr, + crt, + dlt, + dsp. Oprávnění + alladm je ekvivalentní s + chg + clr + dlt + dsp.

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.

Procedura

- Pro systémy UNIX, Linux a Windows zadejte tento příkaz:

```
setmqaut -m QMgrName -n ObjectProfile -t namelist -g GroupName ReqdAction
```

- 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:

– V systémech UNIX, Linux a Windows se všechny kombinace následujících autorizací: + chg, + clr, + crt, + dlt, + ctrl, + ctrlx, + dsp. Oprávnění + alladm je ekvivalentní s + chg + clr + dlt + dsp.

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.

Poznámka: Objekty služby v produktu z/OSneexistují.

Procedura

- Pro systémy UNIX, Linux a Windows zadejte tento příkaz:

```
setmqaut -m QMgrName -n ObjectProfile -t service -g GroupName ReqdAction
```

- Pro IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*SVC) USER(GroupName) AUT(ReqdAction)
MQMNAME('QMgrName')
```

Výsledky

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:

- V systémech UNIX, Linux a Windows se všechny kombinace následujících autorizací: + chg, + clr, + crt, + dlt, + ctrl, + ctrlx, + dsp. Oprávnění + alladm je ekvivalentní s + chg + clr + dlt + dsp.

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 15. 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 170 .
Témata	Udělte úplný administrativní přístup k požadovaným tématům, jak je popsáno v tématu “Udělení úplného administrativního přístupu k některým tématům” na stránce 171 .
Kanály	Udělte úplný administrativní přístup k požadovaným kanálům, jak je popsáno v tématu “Udělení úplného administrativního přístupu k některým kanálům” na stránce 171 .
Správce front	Udělte úplný administrativní přístup ke správci front, jak je popsáno v tématu “Udělení úplného administrativního přístupu ke správci front” na stránce 172 .
Procesy	Udělte úplný administrativní přístup k požadovaným procesům, jak je popsáno v tématu “Udělení úplného administrativního přístupu k některým procesům” na stránce 172 .
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 173
Služby	Udělte úplný administrativní přístup k požadovaným službám, jak je popsáno v tématu “Udělení úplného administrativního přístupu k některým službám” na stránce 174

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.

Procedura

- Pro systémy UNIX, Linux a Windows zadejte tento příkaz:

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +alladm
```

- Pro IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*Q) USER(GroupName) AUT(*ALLADM) MQMNAME('QMgrName')
```

- Pro operační systém z/OSzadejte následující příkazy:

```
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. V systému z/OSmůže tato hodnota představovat také název 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.

Procedura

- Pro systémy UNIX, Linux a Windows zadejte tento příkaz:

```
setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName +alladm
```

- Pro IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*TOPIC) USER(GroupName) AUT(ALLADM)
MQMNAME('QMgrName')
```

- Pro operační systém z/OSzadejte následující příkazy:

```
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. V systému z/OSmůže tato hodnota představovat také název 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.

Procedura

- Pro systémy UNIX, Linux a Windows zadejte tento příkaz:

```
setmqaut -m QMgrName -n ObjectProfile -t channel -g GroupName +alladm
```

- Pro IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*CHL) USER(GroupName) AUT(ALLADM) MQMNAME('QMgrName')
```

- Pro operační systém z/OSzadejte následující příkazy:

```
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. V systému z/OSmůže tato hodnota představovat také název 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.

Procedura

- Pro systémy UNIX, Linux a Windows zadejte tento příkaz:

```
setmqaut -m QMgrName -t qmgr -g GroupName +alladm
```

- Pro IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*MQM) USER(GroupName) AUT(*ALLADM) MQMNAME('QMgrName')
```

- Pro operační systém z/OSzadejte následující příkazy:

```
RDEFINE MQADMIN QMgrName.QMGR UACC(NONE)
PERMIT QMgrName.QMGR CLASS(MQADMIN) ID(GroupName ) ACCESS(ALTER)
```

Názvy proměnných mají následující význam:

QMgrName
Název správce front. V systému z/OSmůže tato hodnota představovat také název 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.

Procedura

- Pro systémy UNIX, Linux a Windows zadejte tento příkaz:

```
setmqaut -m QMgrName -n ObjectProfile -t process -g GroupName +alladm
```

- Pro IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*PRC) USER(GroupName) AUT(*ALLADM) MQMNAME('QMgrName')
```

- Pro operační systém z/OSzadejte následující příkazy:

```
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. V systému z/OSmůže tato hodnota představovat také název 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.

Procedura

- Pro systémy UNIX, Linux a Windows zadejte tento příkaz:

```
setmqaut -m QMgrName -n ObjectProfile -t namelist -g GroupName +alladm
```

- Pro IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*NMLIST) USER(GroupName) AUT(*ALLADM)
MQMNAME('QMgrName')
```

- Pro operační systém z/OSzadejte následující příkazy:

```
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. V systému z/OSmůže tato hodnota představovat také název 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.

Procedura

- Pro systémy UNIX, Linux a Windows zadejte tento příkaz:

```
setmqaut -m QMgrName -n ObjectProfile -t service -g GroupName +alladm
```

- Pro IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*SVC) USER(GroupName) AUT(*ALLADM) MQMNAME('QMgrName')
```

- Pro operační systém z/OSzadejte následující příkazy:

```
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. V systému z/OSmůže tato hodnota představovat také název 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 pouze pro čtení ke všem prostředkům ve správci front

Udělte přístup pouze pro čtení ke všem prostředkům ve správci front, každému uživateli nebo skupině uživatelů, kteří pro ni potřebují obchodní potřeby.

Informace o této úloze

Použijte průvodce Přidání oprávnění založených na rolích nebo příslušné příkazy pro váš operační systém.

Procedura

- Pomocí průvodce:
  a) V podokně WebSphere MQ Explorer Navigator klepněte 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.
- Pro systémy UNIX a 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
setmqaut -m QMgrName -n ** -t topic -g GroupName +dsp
setmqaut -m QMgrName -n ** -t channel -g GroupName +dsp +inq
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
```

Určitá oprávnění k SYSTEM.ADMIN.COMMAND.QUEUE a SYSTEM.MQEXPLORER.REPLY.MODEL je nezbytný pouze v případě, že chcete použít program Průzkumník MQ .

- Pro 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')
```

- Pro operační systém z/OSzadejte následující příkazy:

```
RDEFINE MQQUEUE QMgrName.** UACC(NONE)
PERMIT QMgrName.** CLASS(MQQUEUE) ID(GroupName) ACCESS(READ)
RDEFINE MQTOPIC QMgrName.** UACC(NONE)
PERMIT QMgrName.** CLASS(MQTOPIC) 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. V systému z/OSmůže tato hodnota představovat také název skupiny sdílení front.

GroupName
Název skupiny, ke 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

Použijte průvodce Přidání oprávnění založených na rolích nebo příslušné příkazy pro váš operační systém.

Procedura

- Pomocí průvodce:
  a) V podokně WebSphere MQ Explorer Navigator klepněte 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.
- Pro systémy UNIX 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.QUEUE -t queue -g GroupName +dsp +inq +get
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 +conn
```

- U systémů Windows zadejte stejné příkazy jako pro systémy UNIX and Linux , ale použijte název profilu @CLASS místo @class.
- Pro IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ(*ALL) OBJTYPE(*ALL) USER('GroupName') AUT(*ALLADM) MQMNAME('QMgrName')
```

- Pro operační systém z/OSzadejte následující příkazy:

```
RDEFINE MQADMIN QMgrName.*.** UACC(NONE)
PERMIT QMgrName.*.** CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

Názvy proměnných mají následující význam:

QMgrName
Název správce front. V systému z/OSmůže tato hodnota představovat také název 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.

Procedura

- Pro systémy UNIX, Linux a Windows zadejte tento příkaz:

```
setmqaut -m QMgrName -t qmgr -g GroupName -connect
```

- Pro IBM izadejte tento příkaz:

```
RVKMQMAUT OBJ ('QMgrName') OBJTYPE(*MQM) USER(*ALL) AUT(*CONNECT)
```

- Pro operační systém z/OSzadejte následující příkazy:

```
RDEFINE MQCONN QMgrName.BATCH UACC(NONE)
RDEFINE MQCONN QMgrName.CHIN UACC(NONE)
RDEFINE MQCONN QMgrName.CICS UACC(NONE)
RDEFINE MQCONN QMgrName.IMS UACC(NONE)
```

Nevystavujte žádné příkazy PERMIT.

Názvy proměnných mají následující význam:

QMgrName
Název správce front. V systému z/OSmůže tato hodnota představovat také název 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 184.

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 177.

V obou případech nastavte zabezpečení připojení podle popisu v části “Nastavení zabezpečení připojení” na stránce 184 .

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 185
Máte aplikace, které využívají témata	Viz “Řízení přístupu uživatelů k tématům” na stránce 189.
Máte aplikace, které se dotazujete na objekt správce front	Viz “Udělení oprávnění k dotazům na správce front” na stránce 191.
Máte aplikace, které používají objekty procesu	Viz “Udělení oprávnění pro přístup k procesům” na stránce 191
Máte aplikace, které používají seznamy názvů	Viz “Udělení oprávnění pro přístup k seznamům názvů” na stránce 192

Zabezpečení vzdáleného připojení ke správci front

Vzdálenou připojitelnost ke správci front můžete zabezpečit pomocí zabezpečení SSL nebo 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 SSL nebo 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 SSL nebo 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 SSL, které obdrží v polích SSLPeerNamePtr a SSLPeerNameLength předaných do uživatelské procedury ve struktuře MQCD.

3. Použití SSL nebo 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 SSL nebo 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 ADDRESSMAP, chcete-li dodat jednu adresu nebo adresu zástupného znaku. 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 178
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 143. Další informace o příkazu *MQADMINnaleznete 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. Určíte-li název kanálu připojení serveru v níže uvedených 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 uživatelem deklarovaného ID uživatele na ID uživatele MCAUSER
Záznam ověření kanálu můžete použít ke změně atributu MCAUSER kanálu připojení serveru podle původního 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 asserted klientem.

  user je ID uživatele, které má být použito místo jména uživatele klienta.

Související odkazy
SET CHLAUTH

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
) 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 WebSphere MQ pro hodnoty SSLPEER. Viz pravidla WebSphere MQ pro hodnoty SSLPEER.

uživatel je ID uživatele, které má být použito pro všechna připojení používající zadané DN.

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. Určíte-li název kanálu připojení serveru v níže uvedeném příkazu, 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 deklarovaný ID uživatele klienta

Záznam ověření kanálu můžete použít, chcete-li klientovi zabránit, aby se ID uživatele uplatnil od spuštění 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 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 asserted klientem.

Související odkazy
SET CHLAUTH

Blokování přístupu pro rozlišující název SSL
Záznam ověření kanálu můžete použít k zabránění tomu, aby se rozlišující název zabezpečení SSL spouštěla z 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')
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 WebSphere MQ pro hodnoty SSLPEER. Viz pravidla WebSphere MQ pro hodnoty SSLPEER.

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.

Procedura
- Pro systémy UNIX, Linux a Windows zadejte tento příkaz:

```
setmqaut -m QMgrName -t qmgr -g GroupName +connect
```

- Pro IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ('QMgrName') OBJTYPE(*MQM)  USER('GroupName') AUT(*CONNECT)
```

- Pro operační systém z/OSzadejte následující příkazy:

```
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 dávkovému zpracování, 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 tato hodnota představovat také název skupiny sdílení front.

ObjectProfile
Název objektu nebo generický profil, pro které chcete změnit autorizace.

GroupName
Název skupiny, ke které má být udělen přístup.

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 185
Kontext sady aplikací	Viz “Udělení oprávnění pro nastavení kontextu” na stránce 186
Aplikace předává kontext	Viz “Udělení oprávnění pro předání kontextu” na stránce 186
Aplikace ukládá zprávy do klastrované fronty.	Viz “Autorizace vkládání zpráv ve vzdálených frontách klastru” na stránce 240
Aplikace vkládá zprávy do lokální fronty	Viz “Udělení oprávnění k vkládání zpráv do lokální fronty” na stránce 187
Aplikace vkládá zprávy do modelové fronty	Viz “Udělení oprávnění k vkládání zpráv do modelové fronty” na stránce 188
Aplikace vkládá zprávy do vzdálené fronty	Viz “Udělení oprávnění pro vkládání zpráv do vzdálené fronty klastru” na stránce 188

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.

Procedura

- Pro systémy UNIX, Linux a Windows zadejte tento 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 operační systém z/OSzadejte následující příkazy:

```
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
```

Názvy proměnných mají následující význam:

QMgrName
Název správce front. V systému z/OSmůže tato hodnota představovat také název 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.

Procedura

- Pro systémy UNIX, Linux a 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
    ```

- 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 operační systém 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 tato hodnota představovat také název 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.

Procedura

- Pro systémy UNIX, Linux a 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
    ```

- 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')
    ```

- V případě systému z/OSzadejte kontext identity nebo celý kontext zadáním následujících příkazů:

  ```
  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 tato hodnota představovat také název 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.

Procedura

- Pro systémy UNIX, Linux a Windows zadejte tento 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 operační systém z/OSzadejte následující příkazy:

  ```
  RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
  PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
  ```

  Názvy proměnných mají následující význam:

QMgrName
Název správce front. V systému z/OSmůže tato hodnota představovat také název 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.

Procedura

- Pro systémy UNIX, Linux a 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 operační systém z/OSzadejte následující příkazy:

```
RDEFINE MQQUEUE QMgrName.ModelQueueName UACC(NONE)
PERMIT QMgrName.ModelQueueName CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
```

  Názvy proměnných mají následující význam:

  QMgrName
  Název správce front. V systému z/OSmůže tato hodnota představovat také název 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 do lokálního objektu: viz “Udělení oprávnění k vkládání zpráv do lokální fronty” na stránce 187. 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 systémech UNIX, Linuxa Windows můžete také použít příkaz SET AUTHREC.

Procedura

- Pro systémy UNIX, Linux a Windows zadejte tento 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 operační systém z/OSzadejte následující příkazy:

```
RDEFINE MQQUEUE  QMgrNameObjectProfile UACC(NONE)
PERMIT QMgrNameObjectProfile CLASS(MQADMIN)
ID(GroupName) ACCESS(UPDATE)
```

  Nezapomeňte, že je možné použít název vzdáleného správce front (nebo skupiny sdílení front) pouze pro fronty vzdáleného klastru.

  Názvy proměnných mají následující význam:

  QMgrName
  Název správce front. V systému z/OSmůže tato hodnota představovat také název 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 16. Řízení přístupu uživatelů k tématům

Příkaz	**Akce**
Aplikace publikuje zprávy do tématu	Viz “Udělení oprávnění pro publikování zpráv do tématu” na stránce 189
Aplikace se přihlásí k odběru tématu.	Viz “Udělení oprávnění k odběru témat” na stránce 190

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.

Procedura

- Pro systémy UNIX, Linux a Windows zadejte tento 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 operační systém z/OSzadejte následující příkazy:

```
RDEFINE MQTOPIC QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQTOPIC) ID(GroupName) ACCESS(UPDATE)
```

Názvy proměnných mají následující význam:

QMgrName
Název správce front. V systému z/OSmůže tato hodnota představovat také název 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.

Procedura

- Pro systémy UNIX, Linux a Windows zadejte tento 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 operační systém z/OSzadejte následující příkazy:

```
RDEFINE MQTOPIC QMgrName.SUBSCRIBE.ObjectProfile UACC(NONE)
PERMIT QMgrName.SUBSCRIBE.ObjectProfile CLASS(MQTOPIC) ID(GroupName) ACCESS(UPDATE)
```

Názvy proměnných mají následující význam:

QMgrName
Název správce front. V systému z/OSmůže tato hodnota představovat také název 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.

Procedura

- Pro systémy UNIX, Linux a Windows zadejte tento 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 operační systém z/OSzadejte následující příkazy:

```
RDEFINE MQCMDS QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName ObjectProfile CLASS(MQCMDS) ID(GroupName ) ACCESS(READ)
```

Tyto příkazy udělují přístup k 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 tato hodnota představovat také název 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.

Procedura

- Pro systémy UNIX, Linux a Windows zadejte tento 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 operační systém z/OSzadejte následující příkazy:

```
RDEFINE MQPROC QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQPROC) ID(GroupName) ACCESS(READ)
```

  Názvy proměnných mají následující význam:

  QMgrName
  Název správce front. V systému z/OSmůže tato hodnota představovat také název 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.

Procedura

- Pro systémy UNIX, Linux a Windows zadejte tento 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 operační systém z/OSzadejte následující příkazy:

```
RDEFINE MQNLIST
QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile
 CLASS(MQNLIST) ID(GroupName) ACCESS(READ)
```

  Názvy proměnných mají následující význam:

  QMgrName
  Název správce front. V systému z/OSmůže tato hodnota představovat také název skupiny sdílení front.

  ObjectProfile
  Název objektu nebo generický profil, pro které chcete změnit autorizace.

  GroupName
  Název skupiny, ke které má být udělen přístup.

Oprávnění k administraci produktu IBM WebSphere MQ v systémech UNIX, Linux, and Windows

Administrátoři produktu IBM WebSphere MQ mohou používat všechny příkazy produktu IBM WebSphere 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 WebSphere MQ mají oprávnění k použití všech příkazů produktu WebSphere MQ (včetně příkazů pro udělení oprávnění produktu WebSphere MQ pro ostatní uživatele)

Chcete-li být administrátorem produktu IBM WebSphere MQ , musíte být členem speciální skupiny s názvem skupina *mqm* (nebo členem skupiny Administrators v systémech Windows). Skupina mqm se vytvoří automaticky při instalaci produktu WebSphere MQ ; přidejte další uživatele do skupiny a umožní jim 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 k administraci produktu WebSphere MQ. Jeden z těchto řídicích příkazů je **setmqaut**, který se používá k udělení oprávnění jiným uživatelům, aby jim umožnili přístup k prostředkům produktu WebSphere MQ nebo jejich řízení. Příkazy PCF pro správu záznamů oprávnění jsou k dispozici uživatelům bez oprávnění administrátora, kteří byli ve správci front udělovali příkazy dsp a chg. Další informace o správě oprávnění pomocí příkazů PCF najdete v tématu Programovatelné formáty příkazů.

Administrátoři mohou použít řídicí příkaz **runmqsc** k vydání příkazu IBM WebSphere 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. Administrátoři musí mít požadovaná oprávnění pro příkazy MQSC, které mají být zpracovány vzdáleným správcem front. Produkt WebSphere MQ Explorer vydává příkazy PCF pro provádění administrativních úloh. Administrátoři nevyžadují žádné další oprávnění k administraci správce front v lokálním systému pomocí programu Průzkumník produktu WebSphere MQ . Pokud se Průzkumník IBM WebSphere MQ používá ke správě správce front v jiném systému, administrátoři musí mít požadovaná oprávnění pro příkazy PCF, které mají být zpracovány vzdáleným správcem front.

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 produktu WebSphere 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

Navíc v systémech Windows má účet SYSTEM úplný přístup k prostředkům produktu WebSphere MQ .

Na platformách UNIX and Linux je rovněž vytvořeno speciální ID uživatele mqm, které je možné použít pouze pro produkt. Nesmí být nikdy k dispozici pro neprivilegované uživatele. Všechny objekty produktu WebSphere MQ jsou vlastněny uživatelem ID mqm.

V systémech Windows mohou členové skupiny administrátorů také spravovat libovolného správce front, jako je například účet SYSTEM. Můžete také vytvořit skupinu mqm mqm na řadiči domény, která obsahuje všechna privilegovaná jména uživatelů aktivní v rámci domény, a přidat ji do lokální skupiny mqm. Některé příkazy, například **crtmqm**, manipulují s oprávněními u objektů IBM WebSphere 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” na stránce 197.

Verze systému Windows s funkcí UAC (User Account Control) omezují 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 skupině mqm, musíte použít zvýšený příkazový řádek k zadání příkazů administrátora produktu WebSphere MQ , jako je například **crtmqm**, jinak dojde k chybě "AMQ7077: Nemáte autorizaci 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 69).
- Vydejte volání MQI z aplikačního programu (pokud nechcete použít vazby rychlé cesty na volání MQCONNX).
- Příkaz crtmqcvx se používá k vytvoření fragmentu kódu, který provádí převod dat na strukturách datových typů.
- Chcete-li zobrazit správce front, použijte příkaz dspmq .
- Příkaz dspmqtrc se používá k zobrazení formátovaného výstupu trasování produktu WebSphere MQ .

Omezení 12 znaků se týká jak skupin, tak ID uživatelů.

Platformy UNIX and Linux obecně omezují délku ID uživatele na 12 znaků. Produkt AIX verze 5.3 tento limit zvýšil, ale produkt WebSphere MQ i nadále sleduje omezení znaků 12 znaků na všech platformách UNIX and Linux . Použijete-li ID uživatele delší než 12 znaků, nahradí jej produkt WebSphere MQ hodnotou UNKNOWN. Nedefinujte ID uživatele s hodnotou UNKNOWN.

Správa skupiny mqm

Uživatelům v skupině mqm jsou prostřednictvím produktu WebSphere MQudělena úplná administrativní oprávnění. Z tohoto důvodu byste neměli zapisovat aplikace a běžné uživatele do skupiny mqm. Skupina mqm by měla obsahovat pouze účty administrátorů produktu WebSphere MQ .

Tyto úlohy jsou popsány v následujících tématech:

- Vytvoření a správa skupin v systému Windows
- Vytvoření a správa skupin v systému HP-UX
- Vytvoření a správa skupin v systému AIX
- Vytvoření a správa skupin v systému Solaris
- Vytvoření a správa skupin v systému Linux

Pokud váš řadič domény běží v systému Windows 2000 nebo Windows 2003, může administrátor domény nastavit speciální účet pro produkt WebSphere MQ , který má být použit. Tento popis je popsán v tématu Konfigurace účtů produktu WebSphere MQ.

Oprávnění pro práci s objekty IBM WebSphere MQ v systémech UNIX, Linux, and Windows

Všechny objekty jsou chráněny produktem IBM WebSphere 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 WebSphere MQa aplikace musí mít k dispozici oprávnění pro přístup 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 provedení 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 systémech Windows).

Související pojmy

“Oprávnění k administraci produktu IBM WebSphere MQ v systémech UNIX, Linux, and Windows” na stránce 192

Administrátoři produktu IBM WebSphere MQ mohou používat všechny příkazy produktu IBM WebSphere 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 .

Když jsou provedeny kontroly zabezpečení na systémech UNIX, 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 WebSphere MQ poté ověří, zda je ID uživatele autorizováno pro připojení ke správci front, a zachová ID uživatele pro budoucí kontroly.

Uživatelé se nemusí přihlašovat k produktu WebSphere MQ; produkt WebSphere MQ předpokládá, že uživatelé se přihlásili k základnímu operačnímu systému a byli ověřeni tímto způsobem.

Otevření objektu (volání MQOPEN nebo MQPUT1)
K objektům produktu WebSphere MQ lze přistupovat 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 WebSphere 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. To je popsáno v poznámce “1” na stránce 88.

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 byly nalezeny ve stromu témat v rámci stromu témat, k němuž je aplikace odebíraná. 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.

Jak řízení přístupu je implementováno produktem IBM WebSphere MQ na systémech UNIX, Linux, and Windows

Produkt IBM WebSphere MQ používá služby zabezpečení poskytované podkladovým operačním systémem pomocí správce oprávnění k objektu. IBM WebSphere MQ poskytuje příkazy pro vytváření a údržbu seznamů přístupových práv.

Rozhraní pro řízení přístupu, které se nazývá rozhraní služeb autorizace, je součástí produktu WebSphere MQ. Produkt WebSphere 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 části “Prevence kontrol přístupu k zabezpečení v systémech UNIX, Linux, and Windows” na stránce 163). 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 WebSphere MQ pouze v případě, že mají správné oprávnění. “Řízení přístupu k objektům pomocí OAM v systémech UNIX, Linux a Windows” na stránce 155 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 systému Windowspro uživatele ve skupině administrátorů a uživatelé přihlášení s ID SYSTEM. Uživatelský přístup ke frontě nelze změnit.

Produkt WebSphere MQ poskytuje příkazy k vytvoření a údržbě seznamů přístupových práv. Další informace o těchto příkazech najdete v tématu “Řízení přístupu k objektům pomocí OAM v systémech UNIX, Linux a Windows” na stránce 155.

Produkt WebSphere MQ předá požadavek OAM obsahující činitel, název prostředku a typ přístupu. OAM uděluje nebo odmítá přístup na základě seznamu ACL, který spravuje. WebSphere MQ postupuje podle rozhodnutí OAM; pokud OAM nemůže provést rozhodnutí, produkt WebSphere MQ neumožňuje přístup.

Identifikace ID uživatele na systémech UNIX, 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 WebSphere 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 UNIX 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 WebSphere 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 “Autorita kontextu v systémech UNIX, Linux a Windows” na stránce 198. Aplikace nemohou tyto informace měnit, pokud nemají autorizaci ke změně informací o kontextu.

Činitelé a skupiny

Řídicí služby mohou náležet do skupin. Můžete udělit přístup ke konkrétnímu prostředku spíše skupinám než k jednotlivcům, abyste snížili množství požadované administrace. Na systémech UNIX and Linux jsou všechny seznamy řízení přístupu (ACL) založeny na skupinách, ale na systémech Windows jsou ACLS založeny na ID uživatelů a skupinách.

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 je popsán v:

- Vytvoření a správa skupin v systému Windows
- Vytvoření a správa skupin v systému HP-UX
- Vytvoření a správa skupin v systému AIX
- Vytvoření a správa skupin v systému Solaris
- Vytvoření a správa skupin v systému Linux

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 PCF).

Systémy UNIX and Linux

Všechny seznamy ACL jsou založeny na skupinách. Je-li uživateli udělen přístup ke konkrétnímu prostředku, je v seznamu přístupových práv zahrnuta primární skupina 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. Oprávnění ve skupině *nobody* můžete změnit, chcete-li udělit přístup k prostředkům produktu WebSphere MQ uživatelům bez specifických autorizací.

Nedefinujte ID uživatele s hodnotou "UNKNOWN". Hodnota "UNKNOWN" se používá, když je ID uživatele příliš dlouhé, takže libovolné ID uživatele budou používat přístupová oprávnění NEZNÁMÉ.

ID uživatelů mohou obsahovat až 12 znaků a názvy skupin až 12 znaků.

Systémy Windows

Seznamy ACL jsou založeny na ID uživatelů a skupinách. Kontroly jsou stejné jako u systémů UNIX s tím rozdílem, že ID jednotlivých uživatelů lze také zobrazit v seznamu ACL. V různých doménách můžete mít různé uživatele se stejným ID uživatele. WebSphere MQ povoluje, aby ID uživatelů byla kvalifikována názvem domény, takže těmto uživatelům mohou být poskytnuty různé úrovně přístupu.

Název skupiny může volitelně zahrnovat název domény, uvedený v následujících formátech:

```
GroupName@domain
domain\GroupName
```

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 na objektech WebSphere MQ pomocí správce oprávnění k 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.

Identifikátory zabezpečení systému Windows (SID)

Produkt WebSphere MQ v systému Windows používá identifikátor SID, kde je k dispozici. Pokud není zadán identifikátor SID systému Windows spolu s požadavkem na autorizaci, produkt WebSphere MQ identifikuje uživatele na základě samotného jména uživatele, může však dojít k tomu, že bude uděleno nesprávné oprávnění.

Na systémech Windows se používá identifikátor zabezpečení (SID) k doplnění ID uživatele. SID obsahuje informace, které identifikují podrobnosti o účtu celého uživatele na databázi správce účtů zabezpečení systému Windows , kde je uživatel definován. Je-li vytvořena zpráva v produktu WebSphere MQ for Windows, produkt WebSphere MQ uloží identifikátor SID v deskriptoru zpráv. Když produkt WebSphere MQ v systému Windows provede kontrolu 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.)

Je-li SID Okna s požadavkem na autorizaci, WebSphere MQ standardně identifikuje uživatele na základě samotného jména uživatele. 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 WebSphere MQ . Chcete-li tomuto problému předejít, zahrňte do každého požadavku na autorizaci SID. Identifikátor SID je používán produktem WebSphere MQ k vytvoření pověření uživatele.

Chcete-li zadat, že všechny požadavky na autorizaci musí obsahovat SID, použijte `regedit`. Nastavte SecurityPolicy na NTSIDsRequired.

Oprávnění alternativního uživatele na systémech UNIX, Linux a Windows

Můžete uvést, že ID uživatele může použít oprávnění jiného uživatele při přístupu k objektu WebSphere MQ . To se nazývá *oprávnění alternativního uživatele*a můžete ji použít na libovolném objektu WebSphere 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.

Autorita kontextu v systémech UNIX, Linux a Windows

Kontext je informace, která se vztahuje ke konkrétní zprávě a která je obsažena v deskriptoru zpráv, MQMD, který je součástí zprávy. Aplikace mohou určit data kontextu, když se vytvoří buď volání `MQOPEN` , nebo `MQPUT` .

Informace o kontextu se nacházejí ve dvou sekcích:

Sekce Identita
Od koho ta zpráva přišla. Skládá se z polí `UserIdentifier`, `AccountingTokena` `ApplIdentityData` .

Sekce Původ
Místo, odkud zpráva přišla, a kdy byla vložena do fronty. Skládá se z polí `PutApplType`, `PutApplName`, `PutDate`, `PutTimea` `ApplOriginData` .

Aplikace mohou určit data kontextu, když se vytvoří buď volání `MQOPEN` , nebo `MQPUT` . Tato data mohou být vygenerována aplikací, předána dále z jiné zprávy nebo standardně generována správcem front. Například, kontextová data mohou být použita serverovým programem pro kontrolu identity žadatele, testování, zda zpráva přišla z aplikace běžící pod autorizovaným ID uživatele.

Serverový program může použít `UserIdentifier` k určení ID uživatele alternativního uživatele. Kontextovou autorizaci můžete použít k určení, zda uživatel může určit libovolnou z voleb kontextu na libovolném volání `MQOPEN` nebo `MQPUT1` .

Informace o kontextových volbách viz Řízení kontextové informace a Přehled pro MQMD pro 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 WebSphere 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. *MCAUserIdentifier* obsahuje prvních 12 bajtů identifikátoru uživatele MCA. Pokud identifikátor uživatele MCA není prázdný, určuje identifikátor uživatele, který má být použit agentem kanálu zpráv pro autorizaci pro přístup k prostředkům produktu MQ . Ujistěte se, že MCAUSER je na platformě Windows menší než 12 znaků.

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.

V systémech IBM i, UNIX, Linux a Windows , není-li hodnota *MCAUserIdentifier* prázdná, použije správce front hodnotu *MCAUserIdentifier* jako ID uživatele pro kontrolu oprávnění, když se agent MCA pokusí o přístup k prostředkům správce front poté, co je připojen ke správci front. 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.

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 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 straně klienta kanálu MQI neexistuje žádná uživatelská procedura zabezpečení, ID uživatele přidružené k toku aplikací klienta WebSphere MQ 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 klienta WebSphere MQ MQI. 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 v kanálu použit protokol SSL, je rozlišující název partnera předáván 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: Uživatelské aplikace zabezpečení vytvořené před vydáním produktu WebSphere MQ v7.1 mohou vyžadovat aktualizaci. Další informace najdete v tématu Uživatelské programy zabezpečení kanálu.

Ověření uživatele správce oprávnění k objektu WebSphere MQ

Na připojení klienta WebSphere MQ MQI 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 zpráv a za předpokladu, že má alternativní oprávnění uživatele, požádat správce front o použití tohoto ID uživatele pro kontrolu oprávnění při přístupu k prostředkům produktu WebSphere MQ v zastoupení klienta.

Je-li parametr PUTAUT nastaven na CTX (nebo ALTMCA na systému z/OS) v definici kanálu, bude ID uživatele v poli *UserIdentifier* každé příchozí zprávy použito pro kontrolu oprávnění, je-li agent MCA otevřen cílovou frontou.

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 145.

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 prostředků poskytovaných produktem WebSphere 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.

Důvěrnost zpráv

Chcete-li zachovat důvěrnost, zašifrujte zprávy. V produktu WebSphere MQ jsou k dispozici různé metody šifrování zpráv v závislosti na vašich potřebách.

Vaše volba CipherSpec určuje úroveň důvěrnosti, kterou máte.

Potřebujete-li ochranu dat na úrovni aplikací a koncových bodů pro infrastrukturu systému zpráv, můžete použít produkt WebSphere MQ Advanced Message Security pro šifrování zpráv nebo pro zápis vlastní uživatelské procedury rozhraní API nebo ukončení rozhraní API.

Pokud potřebujete šifrovat zprávy pouze v době, kdy jsou transportovány přes kanál, protože máte na svých správcích front dostatečné zabezpečení, můžete použít SSL nebo TLS, nebo můžete napsat vlastní uživatelskou proceduru pro zabezpečení zprávy, ukončit zprávu nebo odesílat a přijímat ukončovací programy.

Další informace o produktu WebSphere MQ Advanced Message Securitynaleznete v tématu “Plánování pro databázi Advanced Message Security” na stránce 62.Použití SSL a TLS s produktem WebSphere MQ je popsáno v “Podpora produktu IBM WebSphere MQ pro zabezpečení SSL a TLS” na stránce 23. Použití ukončovacích programů v šifrování zpráv je popsáno v “Implementace utajení v uživatelských ukončovacích programech” na stránce 220.

Připojení dvou správců front s použitím zabezpečení SSL nebo TLS

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 získat a spravovat digitální certifikáty. V testovacím systému můžete používat certifikáty podepsané sebou samým nebo certifikáty vydané lokální certifikační autoritou (CA). V provozním systému nepoužívejte certifikáty podepsané svým držitelem. Další informace viz ..//zs14140_.dita.

Úplné informace o vytváření a správě certifikátů naleznete v tématu “Práce se SSL nebo TLS na systémech UNIX, Linux, and Windows” na stránce 111.

Tato kolekce témat představuje úlohy zahrnuté do nastavení 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 WebSphere MQ server SSL nebo TLS vždy vyžádá certifikát od klienta.

Notes:

1. V tomto kontextu klient SSL odkazuje na připojení inicializující navázání komunikace.
2. Další podrobnosti viz Slovníček .

Na systémech UNIX, Linux a Windows odešle klient SSL nebo TLS certifikát pouze v případě, že má jeden označený ve správném formátu WebSphere MQ , který je `ibmwebspheremq` následován názvem správce front, který byl změněn na malá písmena. Například pro `QM1`, `ibmwebspheremqqm1`.

Produkt WebSphere MQ používá předponu `ibmwebspheremq` na štítku, aby se předešlo 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 v případě, že je konec kanálu, který se chová jako server SSL nebo TLS, definován buď s parametrem SSLCAUTH nastaveným na hodnotu REQUIRED, nebo s hodnotou parametru SSLPEER. Další informace o připojení správce front anonymně, tj. když klient SSL nebo TLS neodešle certifikát, viz “Spojování dvou správců front s použitím jednosměrného ověření” na stránce 206.

Použití certifikátů s automatickým podpisem pro vzájemné ověření dvou správců front

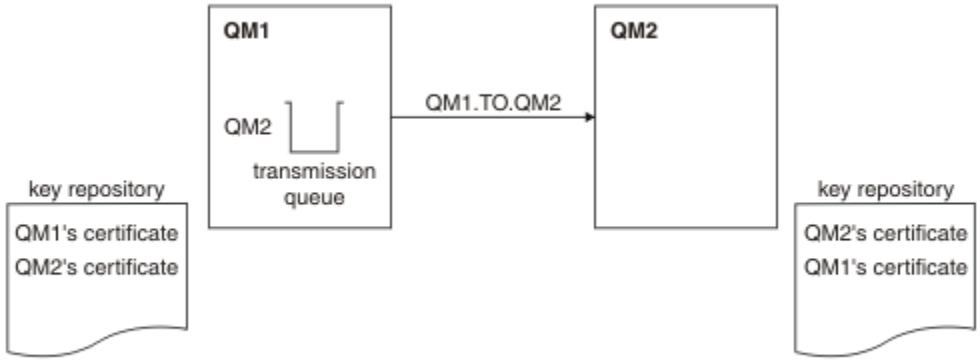
Postupujte podle těchto ukázkových pokynů pro implementaci vzájemného ověření mezi dvěma správci front pomocí certifikátů SSL nebo TLS podepsaných sebou samým.

Informace o této úloze

Scénář:

- K dispozici jsou dva správci front, QM1 a QM2, které potřebují zabezpečenou komunikaci. Požadujete vzájemnou autentizaci, která se má provádět mezi QM1 a QM2.
- Rozhodli jste se otestovat zabezpečenou komunikaci pomocí certifikátů podepsaných sebou samým.

Výsledná konfigurace vypadá takto:



Obrázek 14. Konfigurace vyplývající z této úlohy

V produktu Obrázek 14 na stránce 203obsahuje úložiště klíčů pro QM1 certifikát pro QM1 a veřejný certifikát z QM2. Úložiště klíčů pro QM2 obsahuje certifikát pro QM2 a veřejný certifikát z QM1.

Postup

1. Připravte úložiště klíčů na každém správci front podle operačního systému:
   - Na systémech UNIX, Linuxa Windows.
2. Vytvořte certifikát podepsaný svým držitelem pro každého správce front:
   - Na systémech UNIX, Linuxa Windows.
3. Extrahuje kopii každého certifikátu:
   - Na systémech UNIX, Linuxa Windows.
4. Přeneste veřejnou část certifikátu QM1 na systém QM2 a naopak s pomocí obslužného programu, jako je FTP.
5. Přidejte partnerský certifikát do úložiště klíčů pro každého správce front:
   - Na systémech UNIX, Linuxa Windows.
6. V systému QM1definujte odesílací kanál a asociovanou přenosovou frontu pomocí příkazů, jako je tento příklad:

   ```
   DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(SDR) TRPTYPE(TCP) CONNAME(QM1.MACH.COM) XMITQ(QM2)
   SSLCIPH(RC4_MD5_US) DESCR('Sender channel using SSL from QM1 to QM2')

   DEFINE QLOCAL(QM2) USAGE(XMITQ)
   ```

   Tento příklad používá CipherSpec RC4_MD5. Hodnota CipherSpecs na každém konci kanálu musí být stejná.
7. V systému QM2definujte přijímací kanál zadáním příkazu jako je tento příklad:

   ```
   DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(RCVR) TRPTYPE(TCP) SSLCIPH(RC4_MD5_US)
   SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL from QM1 to QM2')
   ```

   Kanál musí mít stejný název jako odesílací kanál, který jste definovali v kroku 6, a použít stejnou CipherSpec.
8. Spusťte kanál.

Výsledky

Klíčová úložiště a kanály se vytvářejí podle ilustrace v části Obrázek 14 na stránce 203 .

Jak pokračovat dále

Zkontrolujte, zda byla úloha úspěšně dokončena pomocí příkazů DISPLAY. Pokud byla úloha úspěšná, výsledný výstup je podobný výstupu zobrazeným v následujících příkladech.

Ve správci front QM1zadejte následující příkaz:

```
DISPLAY CHS(QM1.TO.QM2) SSLPEER SSLCERTI
```

Výsledný výstup je podobný následujícímu příkladu:

```
DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
     4 : DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(QM1.TO.QM2)                     CHLTYPE(SDR)
   CONNAME(9.20.25.40)                     CURRENT
   RQMNAME(QM2)
   SSLCERTI("CN=QM2,OU=WebSphere MQ Development,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5E:02,CN=QM2,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(MQGET)
   XMITQ(QM2)
```

Ve správci front QM2zadejte následující příkaz:

```
DISPLAY CHS(QM1.TO.QM2) SSLPEER SSLCERTI
```

Výsledný výstup je podobný následujícímu příkladu:

```
DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(QM2.TO.QM1)                     CHLTYPE(RCVR)
   CONNAME(9.20.35.92)                     CURRENT
   RQMNAME(QM1)
   SSLCERTI("CN=QM1,OU=WebSphere MQ Development,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QM1,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
   XMITQ( )
```

Hodnota SSLPEER se v každém případě musí shodovat s hodnotou rozlišujícího názvu v certifikátu partnera, který byl vytvořen v kroku 2. Název vydavatele se shoduje s názvem partnera, protože certifikát je podepsán sám sebou.

SSLPEER je volitelné. Je-li zadán, jeho hodnota musí být nastavena tak, aby bylo povoleno DN v certifikátu partnera (vytvořený v kroku 2). Další informace o použití SSLPEER naleznete v příručce WebSphere MQ rules for SSLPEER values .

Použití certifikátů podepsaných CA pro vzájemné ověření dvou správců front

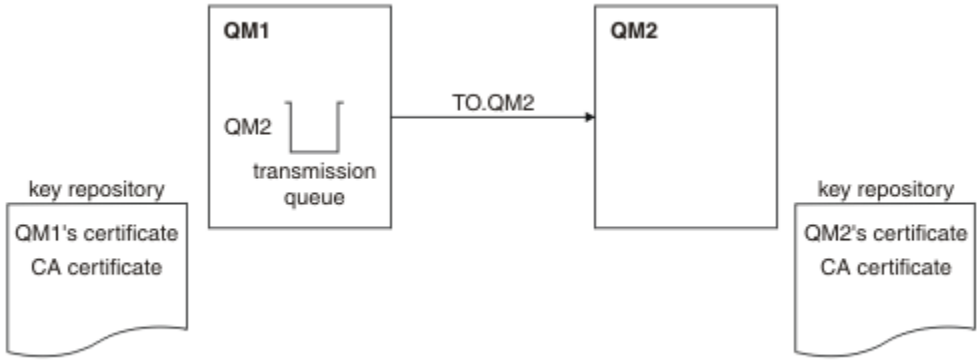
Postupujte podle těchto ukázkových pokynů pro implementaci vzájemného ověření mezi dvěma správci front pomocí certifikátů SSL nebo TLS podepsaných CA.

Informace o této úloze

Scénář:

- K dispozici jsou dva správci front s názvem QMA a QMB, které potřebují zabezpečenou komunikaci. Požadujete vzájemnou autentizaci, která se provede mezi QMA a QMB.
- V budoucnu se chystáte použít tuto síť v provozním prostředí, a proto jste se rozhodli používat certifikáty podepsané CA od začátku.

Výsledná konfigurace vypadá takto:



Obrázek 15. Konfigurace vyplývající z této úlohy

V produktu Obrázek 15 na stránce 205obsahuje úložiště klíčů QMA certifikát QMA a certifikát CA. Úložiště klíčů pro QMB obsahuje certifikát QMB a certifikát CA. V tomto příkladu byl certifikát správce QMA a certifikát QMB vydán stejnou certifikační autoritou. Pokud certifikát QMA a certifikát QMB byly vydány různými CA, pak úložiště klíčů pro QMA a QMB musí obsahovat oba certifikáty CA.

Postup

1. Připravte úložiště klíčů na každém správci front podle operačního systému:
   - Na systémech UNIX, Linuxa Windows.
2. Vyžádejte si certifikát podepsaný CA pro každého správce front.
   Pro dva správce front můžete použít různé CA.
   - Na systémech UNIX, Linuxa Windows.
3. Přidejte certifikát vydavatele certifikátů do úložiště klíčů pro každého správce front:
   Pokud správci front používají různé certifikační autority, musí být certifikát CA pro každou certifikační autoritu přidán do obou úložišť klíčů.
   - Na systémech UNIX, Linuxa Windows.
4. Přidejte certifikát podepsaný CA do úložiště klíčů pro každého správce front:
   - Na systémech UNIX, Linuxa Windows.
5. Na správci QMA definujte odesílací kanál a přidruženou přenosovou frontu pomocí příkazů, jako je tento příklad:

   ```
   DEFINE CHANNEL(TO.QMB) CHLTYPE(SDR) TRPTYPE(TCP) CONNAME(QMB.MACH.COM) XMITQ(QMB)
   SSLCIPH(RC2_MD5_EXPORT) DESCR('Sender channel using SSL from QMA to QMB')

   DEFINE QLOCAL(QMB) USAGE(XMITQ)
   ```

   Tento příklad používá CipherSpec RC4_MD5. Hodnota CipherSpecs na každém konci kanálu musí být stejná.
6. Na QMB definujte přijímací kanál zadáním příkazu jako je tento příklad:

   ```
   DEFINE CHANNEL(TO.QMB) CHLTYPE(RCVR) TRPTYPE(TCP) SSLCIPH(RC2_MD5_EXPORT)
   SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL to QMB')
   ```

   Kanál musí mít stejný název jako odesílací kanál, který jste definovali v kroku 6, a použít stejnou CipherSpec.
7. Spusťte kanál:

Výsledky

Klíčová úložiště a kanály se vytvářejí tak, jak je znázorněno v části Obrázek 15 na stránce 205.

Jak pokračovat dále

Zkontrolujte, zda byla úloha úspěšně dokončena pomocí příkazů DISPLAY. Pokud byla úloha úspěšná, výsledný výstup je podobný výstupu zobrazeným v následujících příkladech.

Ve správci front QMA zadejte tento příkaz:

```
DISPLAY CHS(TO.QMB) SSLPEER SSLCERTI
```

Výsledný výstup je podobný následujícímu příkladu:

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
     4 : DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QMB)                         CHLTYPE(SDR)
   CONNAME(9.20.25.40)                     CURRENT
   RQMNAME(QMB)
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMB,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(MQGET)
   XMITQ(QMB)
```

Z správce front QMB zadejte následující příkaz:

```
DISPLAY CHS(TO.QMB) SSLPEER SSLCERTI
```

Výsledný výstup je podobný následujícímu příkladu:

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QMB)                         CHLTYPE(RCVR)
   CONNAME(9.20.35.92)                     CURRENT
   RQMNAME(QMA)
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMA,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
   XMITQ( )
```

V každém případě musí hodnota SSLPEER odpovídat hodnotě rozlišujícího názvu (DN) v certifikátu partnera, který byl vytvořen v kroku 2. Název vydavatele se shoduje s DN subjektu certifikátu CA, který podepsal osobní certifikát přidaný v kroku 4.

Spojování dvou správců front s použitím jednosměrného ověření

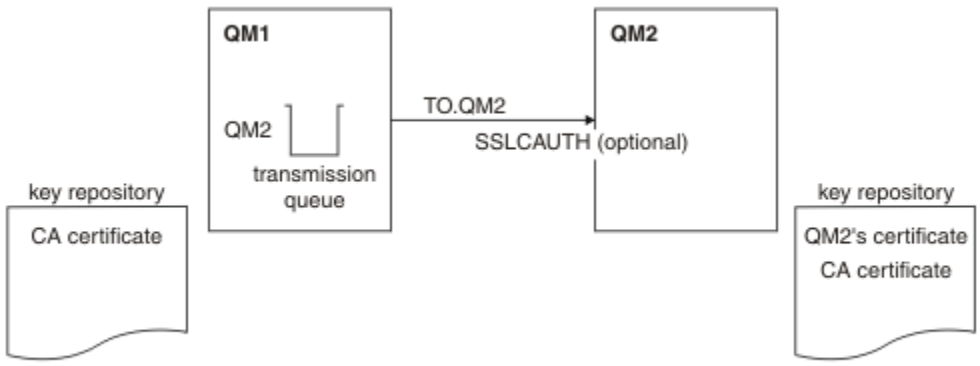
Chcete-li upravit systém se vzájemným ověřením, postupujte podle těchto ukázkových pokynů, které umožní správci front připojit se pomocí jednosměrného ověření k jinému; to znamená, že když klient SSL nebo TLS neodešle certifikát.

Informace o této úloze

Scénář:

- Dva správci front (QM1 a QM2) byli nastavi jako v produktu “Použití certifikátů podepsaných CA pro vzájemné ověření dvou správců front” na stránce 204.
- Chcete změnit QM1 tak, aby se připojoval pomocí jednosměrného ověření k QM2.

Výsledná konfigurace vypadá takto:



Obrázek 16. Správci front povolující jednosměrné ověření

Postup

1. Odeberte osobní certifikát QM1z jeho klíčového úložiště podle operačního systému:
   - Na systémech UNIX, Linuxa Windows. Certifikát je označen takto:
     - `ibmwebspheremq` následovaná názvem vašeho správce front přeloženého na malá písmena. Například pro `QM1` , `ibmwebspheremqqm1`.
2. Volitelné: Pokud v systému QM1dojde k předchozím spuštění jakýchkoli kanálů SSL nebo TLS, aktualizujte prostředí SSL nebo TLS.
3. Povolit anonymní připojení na přijímači.

Výsledky

Klíčová úložiště a kanály se mění podle ilustrace v části Obrázek 16 na stránce 207

Jak pokračovat dále

Pokud byl kanál odesílatele spuštěn a vy jste zadali příkaz REFRESH SECURITY TYPE (SSL) (v kroku 2), kanál se automaticky restartuje. Pokud kanál odesílatele nebyl spuštěn, spusťte jej.

Na konci kanálu je přítomnost hodnoty parametru názvu partnera na obrazovce stavu kanálu indikuje, že došlo k přetečení certifikátu klienta.

Zadáním některých příkazů DISPLAY ověřte, zda byla úloha úspěšně dokončena. Pokud byla úloha úspěšná, výsledný výstup je podobný jako ten, který je zobrazen v následujících příkladech:

Ve správci front QM1 zadejte tento příkaz:

```
DISPLAY CHS(TO.QM2) SSLPEER SSLCERTI
```

Výsledný výstup bude vypadat podobně jako v následujícím příkladu:

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
     4 : DISPLAY CHSTATUS(TO.QMB) SSLPEER
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QM2)                         CHLTYPE(SDR)
   CONNAME(9.20.25.40)                     CURRENT
   RQMNAME(QM2)
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMB,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(MQGET)
   XMITQ(QM2)
```

Ve správci front QM2 zadejte tento příkaz:

```
DISPLAY CHS(TO.QM2) SSLPEER SSLCERTI
```

Výsledný výstup bude vypadat podobně jako v následujícím příkladu:

```
DISPLAY CHSTATUS(TO.QM2) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(TO.QM2) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QM2)                         CHLTYPE(RCVR)
   CONNAME(9.20.35.92)                     CURRENT
   RQMNAME(QMA)                            SSLCERTI( )
   SSLPEER( )                              STATUS(RUNNING)
   SUBSTATE(RECEIVE)                       XMITQ( )
```

V systému QM2je pole SSLPEER prázdné, což znamená, že rozhraní QM1 neodeslala certifikát. V systému QM1hodnota SSLPEER odpovídá hodnotě rozlišujícího názvu DN v osobním certifikátu QM2.

Bezpečná připojení klienta ke správci front

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 získat a spravovat digitální certifikáty. V testovacím systému můžete používat certifikáty podepsané sebou samým nebo certifikáty vydané lokální certifikační autoritou (CA). V provozním systému nepoužívejte certifikáty podepsané svým držitelem. Další informace viz ..//zs14140_.dita.

Úplné informace o vytváření a správě certifikátů naleznete v tématu “Práce se SSL nebo TLS na systémech UNIX, Linux, and Windows” na stránce 111.

Tato kolekce témat představuje úlohy zahrnuté do nastavení 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 WebSphere MQ server SSL nebo TLS vždy vyžádá certifikát od klienta.

U systémů UNIX, Linux, and Windows klient SSL nebo TLS odešle certifikát pouze v případě, že má jeden označený ve správném formátu WebSphere MQ , který je `ibmwebspheremq` následován vaším přihlašovacím ID uživatele, který se změnil na malá písmena, například `ibmwebspheremqmyuserid`.

Produkt WebSphere MQ používá předponu `ibmwebspheremq` na štítku, aby se předešlo 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 v případě, že je konec kanálu, který se chová jako server SSL nebo TLS, definován buď s parametrem SSLCAUTH nastaveným na hodnotu REQUIRED, nebo s hodnotou parametru SSLPEER. Další informace o anonymnímu připojení správce front najdete v tématu “Anonymní připojení klienta ke správci front” na stránce 212.

Použití certifikátů podepsaných sebou samým pro vzájemné ověření klienta a správce front

Chcete-li implementovat vzájemné ověření mezi klientem a správcem front pomocí podepsaných certifikátů SSL nebo TLS, postupujte podle těchto ukázkových instrukcí.

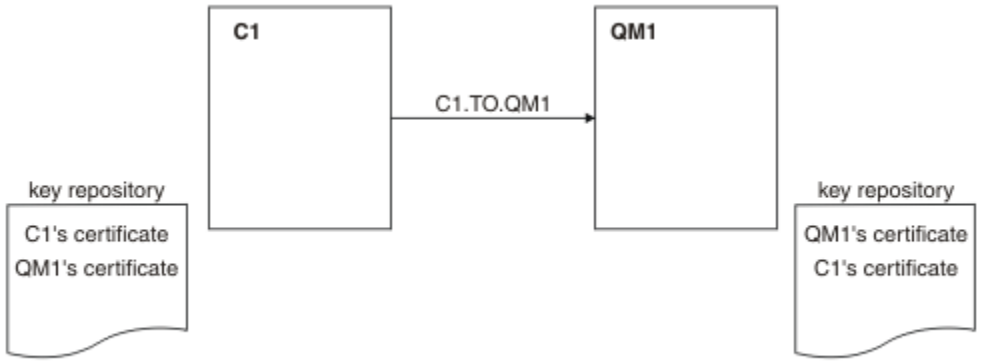
Informace o této úloze

Scénář:

- Máte klienta, C1, a správce front QM1, který musí komunikovat zabezpečeně. Požadujete vzájemnou autentizaci, která bude provedena mezi C1 a QM1.
- Rozhodli jste se otestovat zabezpečenou komunikaci pomocí certifikátů podepsaných sebou samým.

Produkt DCM v systému IBM i nepodporuje certifikáty s automatickým podpisem, takže tato úloha není použitelná na systémech IBM i .

Výsledná konfigurace vypadá takto:



Obrázek 17. Konfigurace vyplývající z této úlohy

V produktu Obrázek 17 na stránce 209obsahuje úložiště klíčů pro QM1 certifikát pro QM1 a veřejný certifikát z C1. Úložiště klíčů pro C1 obsahuje certifikát pro C1 a veřejný certifikát z QM1.

Postup

1. Připravte úložiště klíčů na klientu a správci front podle operačního systému:
   - Na systémech UNIX, Linuxa Windows.
2. Vytvořte certifikáty podepsané sebou samým pro klienta a správce front:
   - Na systémech UNIX, Linuxa Windows.
3. Extrahuje kopii každého certifikátu:
   - Na systémech UNIX, Linuxa Windows.
4. Přeneste veřejnou část certifikátu C1 na systém QM1 a naopak s použitím obslužného programu, jako je FTP.
5. Přidejte certifikát partnera do úložiště klíčů pro klienta a správce front:
   - Na systémech UNIX, Linuxa Windows.
6. Zadejte příkaz REFRESH SECURITY TYPE (SSL) ve správci front.
7. Definujte kanál připojení klienta jedním z následujících způsobů:
   - Použití volání MQCONNX se strukturou MQSCO na C1, jak je popsáno v tématu Vytvoření kanálu připojení klienta na klientovi WebSphere MQ MQI.
   - Pomocí tabulky definic kanálů klienta, jak je popsáno v tématu Vytvoření připojení serveru a definic připojení klienta na serveru .
8. V systému QM1definujte kanál připojení serveru vyvoláním příkazu, jako je tento příklad:

   ```
   DEFINE CHANNEL(C1.TO.QM1) CHLTYPE(SVRCONN) TRPTYPE(TCP) SSLCIPH(RC4_MD5_US)
   SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL from C1 to QM1')
   ```

   Kanál musí mít stejný název jako kanál připojení klienta, který jste definovali v kroku 6, a použít stejnou položku CipherSpec.

Výsledky

Klíčová úložiště a kanály se vytvářejí podle ilustrace v části Obrázek 17 na stránce 209 .

Jak pokračovat dále

Zkontrolujte, zda byla úloha úspěšně dokončena pomocí příkazů DISPLAY. Pokud byla úloha úspěšná, výsledný výstup je podobný výsledku, který je zobrazen v následujícím příkladu.

Ve správci front QM1zadejte následující příkaz:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
```

Výsledný výstup je podobný následujícímu příkladu:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(C1.TO.QM1)                      CHLTYPE(SVRCONN)
   CONNAME(9.20.35.92)                       CURRENT
   SSLCERTI("CN=QM1,OU=WebSphere MQ Development,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5E:02,CN=QM2,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                           SUBSTATE(RECEIVE)
```

Je volitelné nastavit atribut filtru SSLPEER pro definice kanálu. Je-li nastavena definice kanálu SSLPEER, musí se její hodnota shodovat s DN subjektu v certifikátu partnera, který byl vytvořen v kroku 2. Po úspěšném připojení zobrazí pole SSLPEER ve výstupu DISPLAY CHSTATUS rozlišující název DN certifikátu vzdáleného klienta.

Použití certifikátů podepsaných CA pro vzájemné ověření klienta a správce front

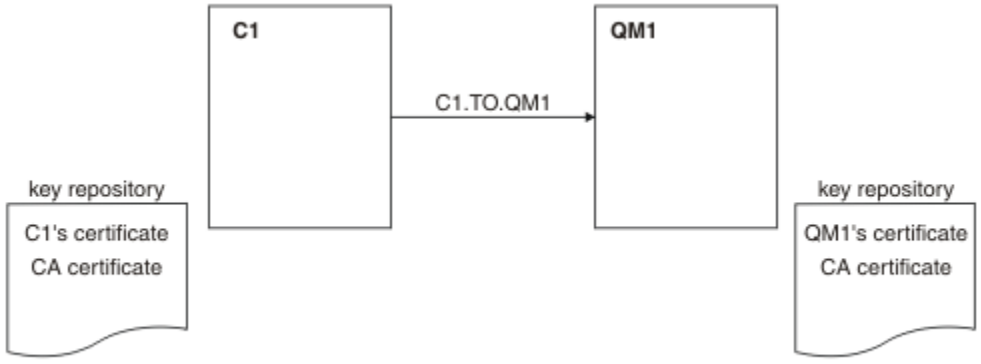
Chcete-li implementovat vzájemné ověření mezi klientem a správcem front pomocí certifikátů SSL nebo TLS, postupujte podle těchto ukázkových instrukcí.

Informace o této úloze

Scénář:

- Máte klienta, C1, a správce front QM1, který musí komunikovat zabezpečeně. Požadujete vzájemnou autentizaci, která bude provedena mezi C1 a QM1.
- V budoucnu se chystáte použít tuto síť v provozním prostředí, a proto jste se rozhodli používat certifikáty podepsané CA od začátku.

Výsledná konfigurace vypadá takto:



Obrázek 18. Konfigurace vyplývající z této úlohy

V produktu Obrázek 18 na stránce 210obsahuje úložiště klíčů pro C1 certifikát pro C1 a certifikát CA. Úložiště klíčů pro QM1 obsahuje certifikát pro QM1 a certifikát CA. V tomto příkladu byl certifikát C1i certifikát QM1vydáván stejným CA. Pokud byl certifikát C1a certifikát QM1vydáván různými CA, pak musí úložiště klíčů C1 a QM1 obsahovat obě certifikáty CA.

Postup

1. Připravte úložiště klíčů na klientu a správci front podle operačního systému:
   - Na systémech UNIX, Linuxa Windows.
2. Vyžádejte si certifikát podepsaný CA pro klienta a správce front.

   Pro klienta a správce front můžete použít různé CA.
   - Na systémech UNIX, Linuxa Windows.
3. Přidejte certifikát vydavatele certifikátů do úložiště klíčů pro klienta a správce front.

   Pokud klient a správce front používají různé certifikační autority, musí být certifikát CA pro každou certifikační autoritu přidán do obou úložišť klíčů.
   - Na systémech UNIX, Linuxa Windows.
4. Přidejte certifikát podepsaný CA do úložiště klíčů pro klienta a správce front:
   - Na systémech UNIX, Linuxa Windows.
5. Definujte kanál připojení klienta jedním z následujících způsobů:
   - Použití volání MQCONNX se strukturou MQSCO na C1, jak je popsáno v tématu Vytvoření kanálu připojení klienta na klientovi WebSphere MQ MQI.
   - Pomocí tabulky definic kanálů klienta, jak je popsáno v tématu Vytvoření připojení serveru a definic připojení klienta na serveru .
6. V systému QM1definujte kanál připojení serveru vyvoláním příkazu, jako je tento příklad:

   ```
   DEFINE CHANNEL(C1.TO.QM1) CHLTYPE(SVRCONN) TRPTYPE(TCP) SSLCIPH(RC2_MD5_EXPORT)
   SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL from C1 to QM1')
   ```

   Kanál musí mít stejný název jako kanál připojení klienta, který jste definovali v kroku 6, a použít stejnou položku CipherSpec.

Výsledky

Klíčová úložiště a kanály se vytvářejí tak, jak je znázorněno v části Obrázek 18 na stránce 210.

Jak pokračovat dále

Zkontrolujte, zda byla úloha úspěšně dokončena pomocí příkazů DISPLAY. Pokud byla úloha úspěšná, výsledný výstup je podobný tomu, který je zobrazen v následujícím příkladu.

Ve správci front QM1zadejte následující příkaz:

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
```

Výsledný výstup je podobný následujícímu příkladu:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(C1.TO.QM1)                      CHLTYPE(SVRCONN)
   CONNAME(9.20.35.92)                     CURRENT
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMA,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
```

Pole SSLPEER ve výstupu DISPLAY CHSTATUS obsahuje DN subjektu certifikátu vzdáleného klienta, který byl vytvořen v kroku 2. Název vydavatele se shoduje s DN subjektu certifikátu CA, který podepsal osobní certifikát přidaný v kroku 4.

Anonymní připojení klienta ke správci front

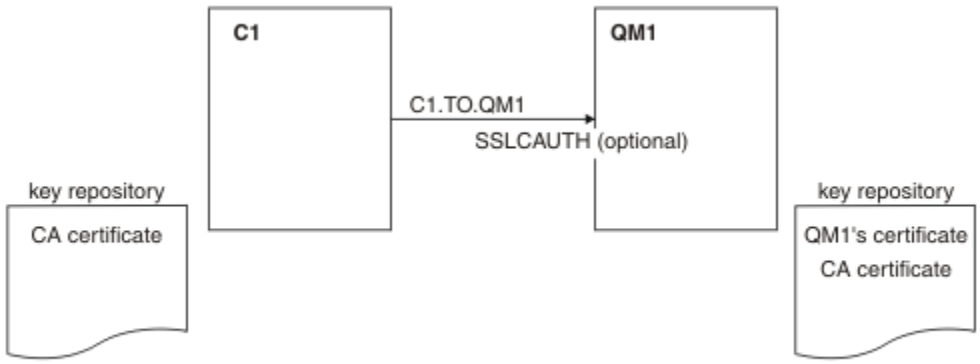
Chcete-li upravit systém se vzájemným ověřováním a umožnit anonymnímu připojení správce front k jinému správci front, postupujte podle těchto ukázkových pokynů.

Informace o této úloze

Scénář:

- Váš správce front a klient (QM1 a C1) byli nastavi jako v produktu “Použití certifikátů podepsaných CA pro vzájemné ověření klienta a správce front” na stránce 210.
- Chcete změnit C1 tak, aby se připojoval anonymně k QM1.

Výsledná konfigurace vypadá takto:



Obrázek 19. Klient a správce front umožňující anonymní připojení

Postup

1. Odeberte osobní certifikát z úložiště klíčů pro C1podle operačního systému:
   - Na systémech UNIX, Linuxa Windows. Certifikát je označen takto:
     - `ibmwebspheremq` následováno vaším ID uživatele pro přihlášení složené do malých písmen, například `ibmwebspheremqmyuserid`.
2. Restartujte aplikaci klienta nebo ukončete aplikaci klienta a znovu otevřete všechna připojení SSL nebo TLS.
3. Povolit anonymní připojení ve správci front zadáním následujícího příkazu:

```
ALTER CHANNEL(C1.TO.QM1) CHLTYPE(SVRCONN) SSLCAUTH(OPTIONAL)
```

Výsledky

Klíčová úložiště a kanály se mění podle ilustrace v části Obrázek 19 na stránce 212

Jak pokračovat dále

Na konci kanálu je přítomnost hodnoty parametru názvu partnera na obrazovce stavu kanálu indikuje, že došlo k přetečení certifikátu klienta.

Zadáním některých příkazů DISPLAY ověřte, zda byla úloha úspěšně dokončena. Pokud byla úloha úspěšná, výsledný výstup je podobný jako v následujícím příkladu:

Ve správci front QM1zadejte následující příkaz:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
```

Výsledný výstup bude vypadat podobně jako v následujícím příkladu:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(C1.TO.QM1)                      CHLTYPE(SVRCONN)
   CONNAME(9.20.35.92)                     CURRENT
   SSLCERTI( )                             SSLPEER( )
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
```

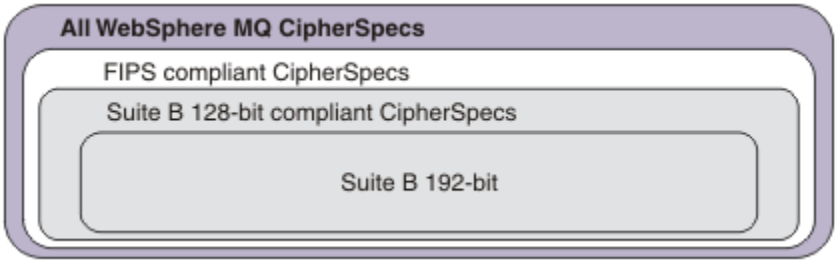
Pole SSLCERTI a SSLPELER jsou prázdná, což ukazuje, že C1 neodeslal certifikát.

Určení CipherSpecs

Zadejte CipherSpec pomocí parametru **SSLCIPH** buď v příkazu **DEFINE CHANNEL** MQSC, nebo v příkazu **ALTER CHANNEL** MQSC.

Některé ze specifikací CipherSpecs , které můžete použít s produktem IBM WebSphere MQ , vyhovují standardu FIPS. Jiné, například NULL_MD5, nejsou. Podobně některé specifikace CipherSpecs odpovídající standardu FIPS jsou také kompatibilní se standardem Suite B, i když jiné kompatibilní 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:



Specifikace šifer, které můžete použít s podporou zabezpečení SSL a TLS systému IBM WebSphere MQ , jsou uvedeny v následující tabulce. Požadujete-li osobní certifikát, určíte velikost klíče pro dvojici veřejný a soukromý klíč. Velikost klíče, která se používá během navázání komunikace SSL, je velikost uložená v certifikátu, pokud není určena CipherSpec, jak je uvedeno v tabulce.

Název specifikace šifrování	Použitý protokol	Algoritmus MAC	Šifrovací algoritmus	Šifrování bitů	FIPS[1]	Sada B 128 bitů	Sada B 192 bitů
NULL_MD5 [a]	SSL 3.0	MD5	Není	0	Ne	Ne	Ne
NULL_SHA [a]	SSL 3.0	SHA-1	Není	0	Ne	Ne	Ne
RC4_MD5_EXPORT [2] [a]	SSL 3.0	MD5	RC4	40	Ne	Ne	Ne
RC4_MD5_US [a]	SSL 3.0	MD5	RC4	128	Ne	Ne	Ne
RC4_SHA_US [a]	SSL 3.0	SHA-1	RC4	128	Ne	Ne	Ne
RC2_MD5_EXPORT [2] [a]	SSL 3.0	MD5	RC2	40	Ne	Ne	Ne
DES_SHA_EXPORT [2] [a]	SSL 3.0	SHA-1	DES	56	Ne	Ne	Ne
RC4_56_SHA_EXPORT1024 [3] [b]	SSL 3.0	SHA-1	RC4	56	Ne	Ne	Ne

Název specifikace šifrování	Použitý protokol	Algoritmus MAC	Šifrovací algoritmus	Šifrování bitů	FIPS[1]	Sada B 128 bitů	Sada B 192 bitů
DES_SHA_EXPORT1024 [3] [b]	SSL 3.0	SHA-1	DES	56	Ne	Ne	Ne
TLS_RSA_WITH_AES_128_CBC_SHA [a]	TLS 1.0	SHA-1	AES	128	Ano	Ne	Ne
TLS_RSA_WITH_AES_256_CBC_SHA [4] [a]	TLS 1.0	SHA-1	AES	256	Ano	Ne	Ne
TLS_RSA_WITH_DES_CBC_SHA [a]	TLS 1.0	SHA-1	DES	56	Č.[5]	Ne	Ne
FIPS_WITH_DES_CBC_SHA [b]	SSL 3.0	SHA-1	DES	56	Č.[6]	Ne	Ne
TLS_RSA_WITH_AES_128_GCM_SHA256 [b]	TLS 1.2	AEAD AES-128 GCM	AES	128	Ano	Ne	Ne
TLS_RSA_WITH_AES_256_GCM_SHA384 [b]	TLS 1.2	AEAD AES-256 GCM	AES	256	Ano	Ne	Ne
TLS_RSA_WITH_AES_128_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES	128	Ano	Ne	Ne
TLS_RSA_WITH_AES_256_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES	256	Ano	Ne	Ne
ECDHE_ECDSA_RC4_128_SHA256 [b]	TLS 1.2	SHA-1	RC4	128	Ne	Ne	Ne
ECDHE_RSA_RC4_128_SHA256 [b]	TLS 1.2	SHA_1	RC4	128	Ne	Ne	Ne
ECDHE_ECDSA_AES_128_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES	128	Ano	Ne	Ne
ECDHE_ECDSA_AES_256_CBC_SHA384 [b]	TLS 1.2	SHA-384	AES	256	Ano	Ne	Ne
ECDHE_RSA_AES_128_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES	128	Ano	Ne	Ne
ECDHE_RSA_AES_256_CBC_SHA384 [b]	TLS 1.2	SHA-384	AES	256	Ano	Ne	Ne
ECDHE_ECDSA_AES_128_GCM_SHA256 [b]	TLS 1.2	AEAD AES-128 GCM	AES	128	Ano	Ano	Ne
ECDHE_ECDSA_AES_256_GCM_SHA384 [b]	TLS 1.2	AEAD AES-256 GCM	AES	256	Ano	Ne	Ano
ECDHE_RSA_AES_128_GCM_SHA256 [b]	TLS 1.2	AEAD AES-128 GCM	AES	128	Ano	Ne	Ne
ECDHE_RSA_AES_256_GCM_SHA384 [b]	TLS 1.2	AEAD AES-256 GCM	AES	256	Ano	Ne	Ne
TLS_RSA_WITH_NULL_SHA256 [b]	TLS 1.2	SHA-256	Není	0	Ne	Ne	Ne
ECDHE_RSA_NULL_SHA256 [b]	TLS 1.2	SHA-1	Není	0	Ne	Ne	Ne
ECDHE_ECDSA_NULL_SHA256 [b]	TLS 1.2	SHA-1	Není	0	Ne	Ne	Ne
TLS_RSA_WITH_NULL_NULL [b]	TLS 1.2	Není	Není	0	Ne	Ne	Ne
TLS_RSA_WITH_RC4_128_SHA256 [b]	TLS 1.2	SHA-1	RC4	128	Ne	Ne	Ne

Název specifikace šifrování	Použitý protokol	Algoritmus MAC	Šifrovací algoritmus	Šifrování bitů	FIPS[1]	Sada B 128 bitů	Sada B 192 bitů

Notes:

1. Uvádí, zda má specifikace šifrování certifikaci FIPS na platformě s certifikací FIPS. Vysvětlení FIPS viz Federal Information Processing Standards (FIPS).
2. 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.
3. Velikost klíče pro navázání komunikace je 1024 bitů.
4. Tuto CipherSpec nelze použít k zabezpečení připojení z produktu WebSphere MQ Explorer ke správci front, pokud nejsou pro prostředí JRE používané průzkumníkem použity příslušné neomezené soubory zásad.
5. Tato specifikace šifrování byla certifikována FIPS 140-2 před 19. květnem 2007.
6. 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.
7. Tuto specifikaci CipherSpec lze použít k přenosu až 32 GB dat, než bude připojení ukončeno chybou AMQ9288. Chcete-li se vyhnout této chybě, při použití této specifikace šifrování nepoužívejte buď algoritmus tripple DES, nebo povolte reset tajného klíče.

Podpora platformy:

- a K dispozici na všech podporovaných platformách.
- b K dispozici pouze na platformách UNIX, Linux, and Windows .

Související pojmy

“Digitální certifikáty a kompatibilita CipherSpec v produktu IBM WebSphere MQ” na stránce 34
Toto téma poskytuje informace o tom, jak vybrat příslušné CipherSpecs a digitální certifikáty pro svou strategii zabezpečení, a to tak, že nastiňují vztah mezi CipherSpecs a digitálními certifikáty v produktu IBM WebSphere MQ.

Související odkazy

Definovat kanál
POZMĚNIT KANÁL

Zamítnuté CipherSpecs

Seznam zamítnutých CipherSpecs , který je v případě potřeby schopen použít produkt WebSphere MQ .

Další informace o tom, jak lze povolit zamítnuté CipherSpecs, naleznete v příručce “Hodnoty CipherSpec podporované v produktu IBM WebSphere MQ” na stránce 38 .

Zamítnuté CipherSpecs , které můžete použít s podporou WebSphere MQ TLS, jsou vypsány v následující tabulce:

Podpora platformy “1” na stránce 217	Název specifikace šifrování	Použitý protokol	Integrita dat	Šifrovací algoritmus	Šifrování bitů	“2” na stránce 217 FIPS	Suite B	Aktualizovat při zamítnutí
Vše	DES_SHA_EXPORT“3” na stránce 217	SSL 3.0	SHA-1	DES	56	Ne	Ne	7.5.0.6

Podpora platformy “1” na stránce 217	Název specifikace šifrování	Použitý protokol	Integrita dat	Šifrovací algoritmus	Šifrovací bitů	“2” na stránce 217 FIPS	Suite B	Aktualizovat při zamítnutí
Windows Linux UNIX	DES_SHA_EXPORT1024“4” na stránce 217	SSL 3.0	SHA-1	DES	56	Ne	Ne	7.5.0.6
Windows Linux UNIX	FIPS_WITH_DES_CBC_SHA	SSL 3.0	SHA-1	DES	56	Ne“6” na stránce 217	Ne	7.5.0.6
Windows Linux UNIX	FIPS_WITH_3DES_EDE_CBC_SHA	SSL 3.0	SHA-1	3DES	168	Ne“7” na stránce 217	Ne	7.5.0.8
Vše	NULL_MD5	SSL 3.0	MD5	Není	0	Ne	Ne	7.5.0.6
Vše	NULL_SHA	SSL 3.0	SHA-1	Není	0	Ne	Ne	7.5.0.6
Vše	RC2_MD5_EXPORT“3” na stránce 217	SSL 3.0	MD5	RC2	40	Ne	Ne	7.5.0.7
Vše	RC4_MD5_EXPORT“3” na stránce 217	SSL 3.0	MD5	RC4	40	Ne	Ne	7.5.0.7
Vše	RC4_MD5_US	SSL 3.0	MD5	RC4	128	Ne	Ne	7.5.0.7
Vše	RC4_SHA_US	SSL 3.0	SHA-1	RC4	128	Ne	Ne	7.5.0.7
Windows Linux UNIX	RC4_56_SHA_EXPORT1024“4” na stránce 217	SSL 3.0	SHA-1	RC4	56	Ne	Ne	7.5.0.7
Vše	TRIPLE_DES_SHA_US	SSL 3.0	SHA-1	3DES	168	Ne	Ne	7.5.0.8
Vše	TLS_RSA_WITH_DES_CBC_SHA	TLS 1.0	SHA-1	DES	56	Ne“5” na stránce 217	Ne	7.5.0.6
Windows Linux UNIX	ECDHE_ECDSA_NULL_SHA256	TLS 1.2	SHA-1	Není	0	Ne	Ne	7.5.0.6
Windows Linux UNIX	ECDHE_ECDSA_RC4_128_SHA256	TLS 1.2	SHA-1	RC4	128	Ne	Ne	7.5.0.7
Windows Linux UNIX	ECDHE_RSA_NULL_SHA256	TLS 1.2	SHA-1	Není	0	Ne	Ne	7.5.0.6
Windows Linux UNIX	ECDHE_RSA_RC4_128_SHA256	TLS 1.2	SHA-1	RC4	128	Ne	Ne	7.5.0.7

Podpora platformy "1" na stránce 217	Název specifikace šifrování	Použitý protokol	Integrita dat	Šifrovací algoritmus	Šifrovací bitů	"2" na stránce 217 FIPS	Suite B	Aktualizovat při zamítnutí
Windows Linux UNIX	TLS_RSA_WITH_NULL_NULL	TLS 1.2	Není	Není	0	Ne	Ne	7.5.0.6
Vše	TLS_RSA_WITH_NULL_SHA256	TLS 1.2	SHA-256	Není	0	Ne	Ne	7.5.0.6
Windows Linux UNIX	TLS_RSA_WITH_RC4_128_SHA256	TLS 1.2	SHA-1	RC4	128	Ne	Ne	7.5.0.7
Vše	TLS_RSA_WITH_3DES_EDE_CBC_SHA"8" na stránce 217	TLS 1.0	SHA-1	3DES	168	Ano	Ne	7.5.0.8
Windows Linux UNIX	ECDHE_ECDSA_3DES_EDE_CBC_SHA256"8" na stránce 217	TLS 1.2	SHA-1	3DES	168	Ano	Ne	7.5.0.8
Windows Linux UNIX	ECDHE_RSA_3DES_EDE_CBC_SHA256"8" na stránce 217	TLS 1.2	SHA-1	3DES	168	Ano	Ne	7.5.0.8

Notes:

1. Pokud není uvedena žádná specifická platforma, je specifikace šifrování dostupná na všech platformách.
2. Uvádí, zda má specifikace šifrování certifikaci FIPS na platformě s certifikací FIPS. Vysvětlení FIPS viz Federal Information Processing Standards (FIPS).
3. 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.
4. Velikost klíče pro navázání komunikace je 1024 bitů.
5. Tato specifikace šifrování byla certifikována FIPS 140-2 před 19. květnem 2007.
6. Tato specifikace šifrování byla certifikována FIPS 140-2 před 19. květnem 2007. Název FIPS_WITH_DES_CBC_SHA je historický a odráží fakt, že tato specifikace šifrování byla dříve v souladu s FIPS (ale už není). Tato specifikace šifrování byla zamítnuta a její použití se nedoporučuje.
7. Název FIPS_WITH_3DES_EDE_CBC_SHA je historický a odráží fakt, že tato specifikace šifrování byla dříve v souladu s FIPS (ale už není). Použití této specifikace šifrování bylo zamítnuto.
8. Tuto specifikaci CipherSpec lze použít k přenosu až 32 GB dat, než bude připojení ukončeno chybou AMQ9288. Chcete-li se vyhnout této chybě, při použití této specifikace šifrování nepoužívejte buď algoritmus tripple DES, nebo povolte reset tajného klíče.

Získání informací o CipherSpecs pomocí produktu IBM WebSphere MQ Explorer

Produkt IBM WebSphere MQ Explorer můžete použít k zobrazení popisů specifikace CipherSpecs.

Chcete-li získat informace o CipherSpecs v produktu "Určení CipherSpecs" na stránce 213, postupujte takto:

1. Otevřete produkt **IBM WebSphere 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.

Alternativy ke specifikaci CipherSpecs

Na těchto platformách, kde operační systém poskytuje podporu zabezpečení SSL, může váš systém podporovat nové specifikace CipherSpecs. Můžete uvést novou CipherSpec s parametrem SSLCIPH, ale hodnota, kterou zadáte, závisí na použité platformě.

Poznámka: Tento oddíl se nevztahuje na systémy UNIX, Linux nebo Windows , protože CipherSpecs jsou dodávány s produktem WebSphere MQ , takže nové CipherSpecs nebudou po odeslání k dispozici.

Na těchto platformách, kde operační systém poskytuje podporu zabezpečení SSL, může váš systém podporovat nové specifikace CipherSpecs , které nejsou zahrnuty v produktu “Určení CipherSpecs” na stránce 213. Můžete uvést novou CipherSpec s parametrem SSLCIPH, ale hodnota, kterou zadáte, závisí na použité platformě. Ve všech případech musí specifikace *odpovídat* odpovídat specifikaci SSL CipherSpec , která je platná a podporovaná verzí protokolu SSL, který systém běží.

IBM i
Dvouznakový řetězec reprezentující hexadecimální hodnotu.

Další informace o povolených hodnotách naleznete v příslušné dokumentaci k produktu (vyhledejte řetězec *cipher_spec* v dokumentaci k produktu IBM i).

Pro uvedení hodnoty můžete použít buď příkaz CHGMQMCHL nebo CRTMQMCHL, například:

```
CRTMQMCHL CHLNAME('channel name') SSLCIPH('hexadecimal value')
```

Chcete-li nastavit parametr SSLCIPH , můžete také použít příkaz ALTER QMGR MQSC.

z/OS
Dvouznakový řetězec reprezentující hexadecimální hodnotu. Hexadecimální kódy odpovídají hodnotám definovaným v protokolu SSL.

Další informace naleznete v popisu rozhraní gsk_environment_open () v kapitole odkazů rozhraní API systému *z/OS Cryptographic Services System SSL Programming*, SC24-5901, kde je uveden seznam všech podporovaných specifikací šifer SSL V3.0 a TLS V1.0 ve formátu dvouciferných hexadecimálních kódů.

Pokyny pro klastry WebSphere MQ

Při použití klastrů WebSphere MQ je nejbezpečnější použít názvy CipherSpec v produktu “Určení CipherSpecs” na stránce 213. Používáte-li alternativní specifikaci, uvědomte si, že specifikace nemusí být platná na jiných platformách. Další informace jsou uvedeny v tématu “SSL a klastry” na stránce 243.

Určení položky CipherSpec pro klienta IBM WebSphere MQ MQI

Existují tři možnosti zadání volby CipherSpec pro klienta IBM WebSphere MQ MQI.

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 třídami IBM WebSphere MQ pro třídy Java a IBM WebSphere MQ pro platformu JMS

Třídy IBM WebSphere MQ pro třídy Java a IBM WebSphere MQ pro platformu JMS specifikují CipherSuites jinak než u jiných platforem.

Informace o určení sady CipherSuite s třídami IBM WebSphere MQ pro jazyk Java naleznete v tématu Podpora zabezpečení SSL (Secure Sockets Layer).

Informace o určení sady CipherSuite s třídami produktu IBM WebSphere MQ pro platformu JMS naleznete v tématu Použití zabezpečení SSL (Secure Sockets Layer) s třídami produktu WebSphere MQ pro službu JMS.

Resetování tajných klíčů SSL a TLS

IBM WebSphere MQ podporuje resetování tajných klíčů na správcích front a klientech.

Tajné klíče jsou resetovány, když byl do kanálu zadán uvedený počet šifrovaných bajtů dat, nebo pokud byl kanál nečinný po určitou dobu.

Hodnota resetování klíče je vždy nastavena na počáteční stranu kanálu MQ .

Správce front

Pro správce front použijte příkaz **ALTER QMGR** s parametrem **SSLRKEYC** k nastavení hodnot použitých během nového vyjednávání klíče.

Klient MQI

Při výchozím nastavení klienti MQI nedohadují tajný klíč. Klienta MQI můžete znovu projednat s novým novým klíčem jedním ze tří způsobů. V následujícím seznamu jsou metody zobrazeny v pořadí podle priority. Pokud zadáte více hodnot, použije se hodnota nejvyšší priority.

1. Použití pole Počet KeyResetve struktuře MQSCO na 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 od 0 do 999 999 999, což představuje počet nezašifrovaných bajtů odeslaných a přijatých v rámci konverzace SSL nebo TLS před opětovným získáním tajného klíče protokolu SSL nebo TLS. Zadání hodnoty 0 označuje, že tajné klíče zabezpečení SSL nebo TLS nejsou nikdy znovu vyjednávány. Zadáte-li počet obnovení tajných klíčů zabezpečení SSL nebo TLS v rozsahu od 1 bajtu do 32 KB, budou kanály SSL nebo TLS používat počet obnovení tajných klíčů 32 kB. Tím se vyhnete nadměrnému resetováním klíčů, které by mohlo nastat pro malé hodnoty resetování tajného klíče SSL nebo TLS.

Je-li zadána hodnota větší než nula a jsou-li pro kanál povoleny prezenční signály kanálu, je tajný klíč také znovu vyjednán před odesláním nebo přijetím dat zprávy po synchronizačním signálu kanálu.

Počet bajtů do obnovení dalšího opětovného domlouvání tajného klíče po každé úspěšné opětovné domlouvání.

Podrobné informace o struktuře MQSCO naleznete v příručce KeyResetCount (MQLONG). Podrobné informace o příkazu MQSSLRESET naleznete v části MQSSLRESET. Další informace o použití zabezpečení SSL nebo TLS v konfiguračním souboru klienta naleznete v tématu Sekce SSL konfiguračního souboru klienta.

Java

V případě produktu IBM WebSphere 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 Hashtable. Aplikace pak přiřadí tabulku hashtable do pole `properties` ve třídě MQEnvironment nebo předá hašovací tabulku objektu MQQueueManager do svého konstruktoru.

Pokud aplikace používá více než jeden z těchto způsobů, použijí se obvyklá pravidla přednosti. Viz Třída com.ibm.mq.MQEnvironment pro pravidla priority.

Hodnota pole sslResetCount nebo vlastnost prostředí MQC.SSL_RESET_COUNT_PROPERTY představuje celkový počet bajtů odeslaných a přijatých kódem klienta WebSphere MQ pro kód klienta Java před opětovným získáním tajného klíče. Počet odeslaných bajtů je číslo před šifrováním a počet přijatých bajtů je číslo po dešifrování. Počet bajtů zahrnuje také řídicí informace odeslané a přijaté třídami WebSphere MQ pro klienta Java.

Pokud je počet obnovení nulový, což je výchozí hodnota, tajný klíč není nikdy znovu vyjednáván. Počet obnovení je ignorován, pokud není zadán parametr CipherSuite .

JMS

Pro produkt IBM WebSphere MQ classes for JMSpředstavuje vlastnost SSLRESETCOUNT celkový počet bajtů odeslaných a přijatých připojením před opětovným získáním tajného klíče, který se používá pro šifrování. Počet odeslaných bajtů je číslo před šifrováním a počet přijatých bajtů je číslo po dešifrování. Počet bajtů obsahuje také řídicí informace odeslané a přijaté produktem IBM WebSphere MQ classes for JMS. Chcete-li například konfigurovat objekt ConnectionFactory , který lze použít k vytvoření připojení prostřednictvím protokolu SSL nebo kanálu MQI s povoleným modulem MQI s utajovaným klíčem, který je znovu vyjednán po 4 MB dat, zadejte pro správce JMSAdmin následující příkaz:

```
ALTER CF(my.cf) SSLRESETCOUNT(4194304)
```

Je-li hodnota parametru SSLRESETCOUNT rovna nule, což je výchozí hodnota, nebude tajný klíč nikdy znovu vyjednáván. Vlastnost SSLRESETCOUNT je ignorována, není-li nastavena hodnota SSLCIPHERSUITE.

.NET

Pro nespravované klienty .NET označuje celočíselné vlastnosti SSLKeyResetpočet počet nezašifrovaných bajtů odeslaných a přijatých v rámci konverzace SSL nebo TLS, než je znovu vyjednán tajný klíč.

Informace o použití vlastností objektu ve třídách IBM WebSphere MQ pro .NET najdete v tématu Získání a nastavení hodnot atributu.

XMS .NET

U nespravovaných klientů rozhraní XMS .NET si přečtěte téma Zabezpečená připojení ke správci front produktu IBM WebSphere MQ.

Související odkazy
ZMĚNIT QMGR
ZOBRAZIT QMGR

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 220.

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.

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 SSL nebo TLS určuje vaše volba CipherSpec úroveň integrity dat v rámci podniku. Používáte-li službu WebSphere MQ Advanced Message Service (AMS), můžete určit 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.

Připojení dvou správců front s použitím zabezpečení SSL nebo TLS

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 získat a spravovat digitální certifikáty. V testovacím systému můžete používat certifikáty podepsané sebou samým nebo certifikáty vydané lokální certifikační autoritou (CA). V provozním systému nepoužívejte certifikáty podepsané svým držitelem. Další informace viz ../zs14140_.dita.

Úplné informace o vytváření a správě certifikátů naleznete v tématu “Práce se SSL nebo TLS na systémech UNIX, Linux, and Windows” na stránce 111.

Tato kolekce témat představuje úlohy zahrnuté do nastavení 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 WebSphere MQ server SSL nebo TLS vždy vyžádá certifikát od klienta.

Notes:

1. V tomto kontextu klient SSL odkazuje na připojení inicializující navázání komunikace.
2. Další podrobnosti viz Slovníček .

Na systémech UNIX, Linux a Windows odešle klient SSL nebo TLS certifikát pouze v případě, že má jeden označený ve správném formátu WebSphere MQ , který je `ibmwebspheremq` následován názvem správce front, který byl změněn na malá písmena. Například pro `QM1`, `ibmwebspheremqqm1`.

Produkt WebSphere MQ používá předponu `ibmwebspheremq` na štítku, aby se předešlo 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 v případě, že je konec kanálu, který se chová jako server SSL nebo TLS, definován buď s parametrem SSLCAUTH nastaveným na hodnotu REQUIRED, nebo s hodnotou parametru SSLPEER. Další informace o připojení správce front anonymně, tj. když klient SSL nebo TLS neodešle certifikát, viz “Spojování dvou správců front s použitím jednosměrného ověření” na stránce 206.

Digitální certifikáty certifikátu, základní informace o požadavcích

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

Informace o této úloze

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 certifikátu *Subject Distinguished Name* nebo *Subject Common Name* . Všimněte si, že pole *Rozlišovací jméno subjektu* a *Obecný název předmětu* jsou pole v rámci certifikátu samotného. Ty jsou definovány při vytvoření certifikátu a nelze je změnit. Můžete však změnit popisek přidružený k digitálnímu certifikátu, je-li to nutné.

Jak se používá jmenovka certifikátu?

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

Štítky certifikátů dodržují konvenci pojmenování; musíte se ujistit, že používáte správnou konvenci pojmenování štítků odpovídající platformě, kterou používáte.

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

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 WebSphere MQ server SSL nebo TLS vždy požaduje certifikát od klienta a klient vždy poskytne certifikát serveru, pokud je nalezen. Pokud klient nemůže najít osobní certifikát, pošle klientovi odpověď no `certificate` na server.

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

Další informace o připojení správce front s použitím jednosměrného ověření, tj. když klient SSL nebo TLS neodešle certifikát, viz “Spojování dvou správců front s použitím jednosměrného ověření” na stránce 206.

, systémy UNIX, Linux, and Windows

Informace o této úloze

Na systémech , UNIX, Linux, and Windows odesílá server SSL nebo TLS certifikát klientovi, pouze tehdy, pokud server najde jeden označený ve správném formátu IBM WebSphere MQ . Na těchto systémech je správný formát `ibmwebspheremq`, za nímž následuje název správce front, který byl změněn na malá písmena.

Například pro správce front s názvem `QM1`je požadavek na jmenovku certifikátu následující:

```
ibmwebspheremqqm1
```

Pokud v úložišti klíčů správce front není nalezen žádný certifikát, který odpovídá požadovanému popisku ve správném formátu případu a formátu, dojde k chybě a navázání komunikace SSL nebo TLS selže.

IBM WebSphere MQ klient

Informace o této úloze

Při připojení z aplikace klienta IBM WebSphere MQ odešle klient SSL nebo TLS certifikát pouze v případě, že má jeden certifikát se jmenovkou ve formátu `ibmwebspheremq`, za nímž následuje jméno uživatele, který spouští proces aplikace klienta.

Například pro jméno uživatele `wasadmin`je požadavek na popisek certifikátu zobrazen tak, jak je složený z malých písmen:

```
  ibmwebspheremqwasadmin
```

Výše uvedený požadavek se vztahuje na služby Message Service Clients for C, C + + a .NET.

IBM WebSphere MQ Java or IBM WebSphere MQ JMS client

Informace o této úloze

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

Výchozí chování je, že klient JSSE iteruje prostřednictvím certifikátů v úložišti klíčů výběrem prvního přijatelného osobního certifikátu. 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 aplikací klienta Java produktu IBM WebSphere MQ v kombinaci se specifickým poskytovatelem JSSE můžete povolit ladění pomocí nastavení.

```
javax.net.debug=ssl
```

v prostředí JVM.

Můžete použít příkaz `-Djavax.net.debug=ssl` na příkazovém řádku nebo nastavit proměnnou v rámci aplikace nebo prostřednictvím konfigurace.

Související pojmy

“Import osobního certifikátu do úložiště klíčů v systémech UNIX, Linux, and Windows” na stránce 130
Chcete-li importovat osobní certifikát, postupujte podle této procedury.

Použití certifikátů s automatickým podpisem pro vzájemné ověření dvou správců front

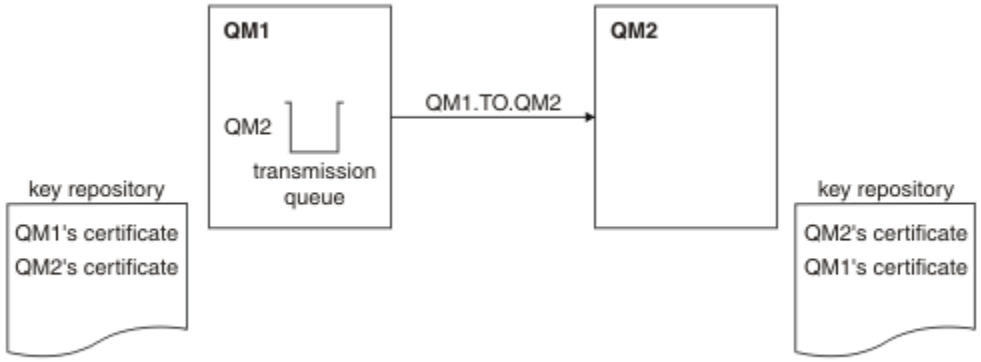
Postupujte podle těchto ukázkových pokynů pro implementaci vzájemného ověření mezi dvěma správci front pomocí certifikátů SSL nebo TLS podepsaných sebou samým.

Informace o této úloze

Scénář:

- K dispozici jsou dva správci front, QM1 a QM2, které potřebují zabezpečenou komunikaci. Požadujete vzájemnou autentizaci, která se má provádět mezi QM1 a QM2.
- Rozhodli jste se otestovat zabezpečenou komunikaci pomocí certifikátů podepsaných sebou samým.

Výsledná konfigurace vypadá takto:



Obrázek 20. Konfigurace vyplývající z této úlohy

V produktu Obrázek 14 na stránce 203obsahuje úložiště klíčů pro QM1 certifikát pro QM1 a veřejný certifikát z QM2. Úložiště klíčů pro QM2 obsahuje certifikát pro QM2 a veřejný certifikát z QM1.

Postup

1. Připravte úložiště klíčů na každém správci front podle operačního systému:
   - Na systémech UNIX, Linuxa Windows.
2. Vytvořte certifikát podepsaný svým držitelem pro každého správce front:
   - Na systémech UNIX, Linuxa Windows.
3. Extrahuje kopii každého certifikátu:
   - Na systémech UNIX, Linuxa Windows.
4. Přeneste veřejnou část certifikátu QM1 na systém QM2 a naopak s pomocí obslužného programu, jako je FTP.
5. Přidejte partnerský certifikát do úložiště klíčů pro každého správce front:
   - Na systémech UNIX, Linuxa Windows.
6. V systému QM1definujte odesílací kanál a asociovanou přenosovou frontu pomocí příkazů, jako je tento příklad:

   ```
   DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(SDR) TRPTYPE(TCP) CONNAME(QM1.MACH.COM) XMITQ(QM2)
   SSLCIPH(RC4_MD5_US) DESCR('Sender channel using SSL from QM1 to QM2')

   DEFINE QLOCAL(QM2) USAGE(XMITQ)
   ```

   Tento příklad používá CipherSpec RC4_MD5. Hodnota CipherSpecs na každém konci kanálu musí být stejná.

7. V systému QM2definujte přijímací kanál zadáním příkazu jako je tento příklad:

```
DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(RCVR) TRPTYPE(TCP) SSLCIPH(RC4_MD5_US)
SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL from QM1 to QM2')
```

   Kanál musí mít stejný název jako odesílací kanál, který jste definovali v kroku 6, a použít stejnou CipherSpec.
8. Spusťte kanál.

Výsledky

Klíčová úložiště a kanály se vytvářejí podle ilustrace v části Obrázek 14 na stránce 203 .

Jak pokračovat dále

Zkontrolujte, zda byla úloha úspěšně dokončena pomocí příkazů DISPLAY. Pokud byla úloha úspěšná, výsledný výstup je podobný výstupu zobrazeným v následujících příkladech.

Ve správci front QM1zadejte následující příkaz:

```
DISPLAY CHS(QM1.TO.QM2) SSLPEER SSLCERTI
```

Výsledný výstup je podobný následujícímu příkladu:

```
DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
     4 : DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(QM1.TO.QM2)                     CHLTYPE(SDR)
   CONNAME(9.20.25.40)                     CURRENT
   RQMNAME(QM2)
   SSLCERTI("CN=QM2,OU=WebSphere MQ Development,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5E:02,CN=QM2,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(MQGET)
   XMITQ(QM2)
```

Ve správci front QM2zadejte následující příkaz:

```
DISPLAY CHS(QM1.TO.QM2) SSLPEER SSLCERTI
```

Výsledný výstup je podobný následujícímu příkladu:

```
DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(QM2.TO.QM1)                     CHLTYPE(RCVR)
   CONNAME(9.20.35.92)                     CURRENT
   RQMNAME(QM1)
   SSLCERTI("CN=QM1,OU=WebSphere MQ Development,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QM1,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
   XMITQ( )
```

Hodnota SSLPEER se v každém případě musí shodovat s hodnotou rozlišujícího názvu v certifikátu partnera, který byl vytvořen v kroku 2. Název vydavatele se shoduje s názvem partnera, protože certifikát je podepsán sám sebou.

SSLPEER je volitelné. Je-li zadán, jeho hodnota musí být nastavena tak, aby bylo povoleno DN v certifikátu partnera (vytvořený v kroku 2). Další informace o použití SSLPEER naleznete v příručce WebSphere MQ rules for SSLPEER values .

Použití certifikátů podepsaných CA pro vzájemné ověření dvou správců front

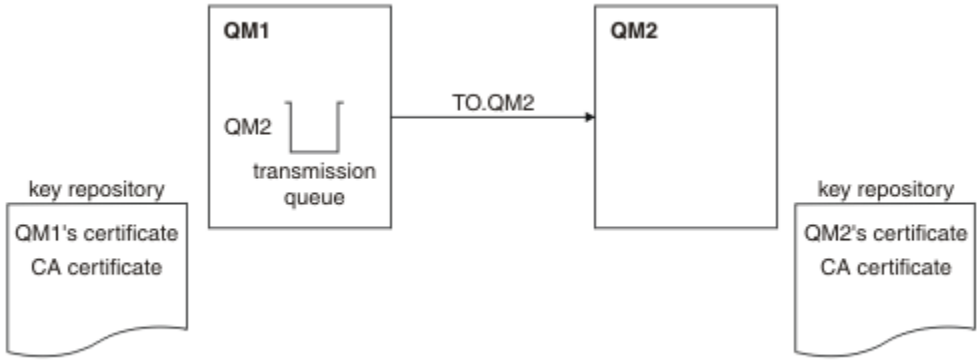
Postupujte podle těchto ukázkových pokynů pro implementaci vzájemného ověření mezi dvěma správci front pomocí certifikátů SSL nebo TLS podepsaných CA.

Informace o této úloze

Scénář:

- K dispozici jsou dva správci front s názvem QMA a QMB, které potřebují zabezpečenou komunikaci. Požadujete vzájemnou autentizaci, která se provede mezi QMA a QMB.
- V budoucnu se chystáte použít tuto síť v provozním prostředí, a proto jste se rozhodli používat certifikáty podepsané CA od začátku.

Výsledná konfigurace vypadá takto:



Obrázek 21. Konfigurace vyplývající z této úlohy

V produktu Obrázek 15 na stránce 205obsahuje úložiště klíčů QMA certifikát QMA a certifikát CA. Úložiště klíčů pro QMB obsahuje certifikát QMB a certifikát CA. V tomto příkladu byl certifikát správce QMA a certifikát QMB vydán stejnou certifikační autoritou. Pokud certifikát QMA a certifikát QMB byly vydány různými CA, pak úložiště klíčů pro QMA a QMB musí obsahovat oba certifikáty CA.

Postup

1. Připravte úložiště klíčů na každém správci front podle operačního systému:
   - Na systémech UNIX, Linuxa Windows.
2. Vyžádejte si certifikát podepsaný CA pro každého správce front.

   Pro dva správce front můžete použít různé CA.
   - Na systémech UNIX, Linuxa Windows.
3. Přidejte certifikát vydavatele certifikátů do úložiště klíčů pro každého správce front:

   Pokud správci front používají různé certifikační autority, musí být certifikát CA pro každou certifikační autoritu přidán do obou úložišť klíčů.
   - Na systémech UNIX, Linuxa Windows.
4. Přidejte certifikát podepsaný CA do úložiště klíčů pro každého správce front:
   - Na systémech UNIX, Linuxa Windows.
5. Na správci QMA definujte odesílací kanál a přidruženou přenosovou frontu pomocí příkazů, jako je tento příklad:

   ```
   DEFINE CHANNEL(TO.QMB) CHLTYPE(SDR) TRPTYPE(TCP) CONNAME(QMB.MACH.COM) XMITQ(QMB)
   SSLCIPH(RC2_MD5_EXPORT) DESCR('Sender channel using SSL from QMA to QMB')

   DEFINE QLOCAL(QMB) USAGE(XMITQ)
   ```

   Tento příklad používá CipherSpec RC4_MD5. Hodnota CipherSpecs na každém konci kanálu musí být stejná.
6. Na QMB definujte přijímací kanál zadáním příkazu jako je tento příklad:

```
DEFINE CHANNEL(TO.QMB) CHLTYPE(RCVR) TRPTYPE(TCP) SSLCIPH(RC2_MD5_EXPORT)
SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL to QMB')
```

Kanál musí mít stejný název jako odesílací kanál, který jste definovali v kroku 6, a použít stejnou CipherSpec.

7. Spusťte kanál:

Výsledky

Klíčová úložiště a kanály se vytvářejí tak, jak je znázorněno v části Obrázek 15 na stránce 205.

Jak pokračovat dále

Zkontrolujte, zda byla úloha úspěšně dokončena pomocí příkazů DISPLAY. Pokud byla úloha úspěšná, výsledný výstup je podobný výstupu zobrazeným v následujících příkladech.

Ve správci front QMA zadejte tento příkaz:

```
DISPLAY CHS(TO.QMB) SSLPEER SSLCERTI
```

Výsledný výstup je podobný následujícímu příkladu:

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
     4 : DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QMB)                         CHLTYPE(SDR)
   CONNAME(9.20.25.40)                     CURRENT
   RQMNAME(QMB)
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMB,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(MQGET)
   XMITQ(QMB)
```

Z správce front QMB zadejte následující příkaz:

```
DISPLAY CHS(TO.QMB) SSLPEER SSLCERTI
```

Výsledný výstup je podobný následujícímu příkladu:

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QMB)                         CHLTYPE(RCVR)
   CONNAME(9.20.35.92)                     CURRENT
   RQMNAME(QMA)
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMA,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
   XMITQ( )
```

V každém případě musí hodnota SSLPEER odpovídat hodnotě rozlišujícího názvu (DN) v certifikátu partnera, který byl vytvořen v kroku 2. Název vydavatele se shoduje s DN subjektu certifikátu CA, který podepsal osobní certifikát přidaný v kroku 4.

Spojování dvou správců front s použitím jednosměrného ověření

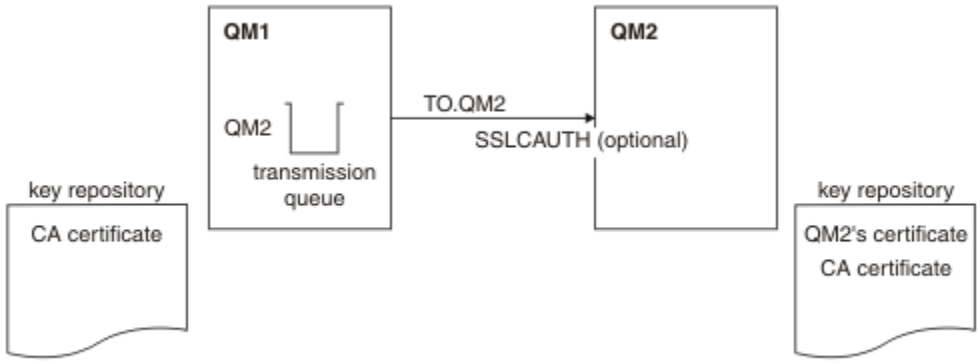
Chcete-li upravit systém se vzájemným ověřením, postupujte podle těchto ukázkových pokynů, které umožní správci front připojit se pomocí jednosměrného ověření k jinému; to znamená, že když klient SSL nebo TLS neodešle certifikát.

Informace o této úloze

Scénář:

- Dva správci front (QM1 a QM2) byli nastavi jako v produktu “Použití certifikátů podepsaných CA pro vzájemné ověření dvou správců front” na stránce 204.
- Chcete změnit QM1 tak, aby se připojoval pomocí jednosměrného ověření k QM2.

Výsledná konfigurace vypadá takto:



Obrázek 22. Správci front povolující jednosměrné ověření

Postup

1. Odeberte osobní certifikát QM1z jeho klíčového úložiště podle operačního systému:
   - Na systémech UNIX, Linuxa Windows. Certifikát je označen takto:
     - `ibmwebspheremq` následovaná názvem vašeho správce front přeloženého na malá písmena. Například pro `QM1` , `ibmwebspheremqqm1`.
2. Volitelné: Pokud v systému QM1dojde k předchozím spuštění jakýchkoli kanálů SSL nebo TLS, aktualizujte prostředí SSL nebo TLS.
3. Povolit anonymní připojení na přijímači.

Výsledky

Klíčová úložiště a kanály se mění podle ilustrace v části Obrázek 16 na stránce 207

Jak pokračovat dále

Pokud byl kanál odesílatele spuštěn a vy jste zadali příkaz REFRESH SECURITY TYPE (SSL) (v kroku 2), kanál se automaticky restartuje. Pokud kanál odesílatele nebyl spuštěn, spusťte jej.

Na konci kanálu je přítomnost hodnoty parametru názvu partnera na obrazovce stavu kanálu indikuje, že došlo k přetečení certifikátu klienta.

Zadáním některých příkazů DISPLAY ověřte, zda byla úloha úspěšně dokončena. Pokud byla úloha úspěšná, výsledný výstup je podobný jako ten, který je zobrazen v následujících příkladech:

Ve správci front QM1 zadejte tento příkaz:

```
DISPLAY CHS(TO.QM2) SSLPEER SSLCERTI
```

Výsledný výstup bude vypadat podobně jako v následujícím příkladu:

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
     4 : DISPLAY CHSTATUS(TO.QMB) SSLPEER
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QM2)                         CHLTYPE(SDR)
   CONNAME(9.20.25.40)                     CURRENT
   RQMNAME(QM2)
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
```

```
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMB,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                          SUBSTATE(MQGET)
   XMITQ(QM2)
```

Ve správci front QM2 zadejte tento příkaz:

```
DISPLAY CHS(TO.QM2) SSLPEER SSLCERTI
```

Výsledný výstup bude vypadat podobně jako v následujícím příkladu:

```
DISPLAY CHSTATUS(TO.QM2) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(TO.QM2) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QM2)                          CHLTYPE(RCVR)
   CONNAME(9.20.35.92)                      CURRENT
   RQMNAME(QMA)                             SSLCERTI( )
   SSLPEER( )                               STATUS(RUNNING)
   SUBSTATE(RECEIVE)                        XMITQ( )
```

V systému QM2je pole SSLPEER prázdné, což znamená, že rozhraní QM1 neodeslala certifikát. V systému QM1hodnota SSLPEER odpovídá hodnotě rozlišujícího názvu DN v osobním certifikátu QM2.

Bezpečná připojení klienta ke správci front

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 získat a spravovat digitální certifikáty. V testovacím systému můžete používat certifikáty podepsané sebou samým nebo certifikáty vydané lokální certifikační autoritou (CA). V provozním systému nepoužívejte certifikáty podepsané svým držitelem. Další informace viz ../zs14140_.dita.

Úplné informace o vytváření a správě certifikátů naleznete v tématu “Práce se SSL nebo TLS na systémech UNIX, Linux, and Windows” na stránce 111.

Tato kolekce témat představuje úlohy zahrnuté do nastavení 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 WebSphere MQ server SSL nebo TLS vždy vyžádá certifikát od klienta.

U systémů UNIX, Linux, and Windows klient SSL nebo TLS odešle certifikát pouze v případě, že má jeden označený ve správném formátu WebSphere MQ , který je `ibmwebspheremq` následován vaším přihlašovacím ID uživatele, který se změnil na malá písmena, například `ibmwebspheremqmyuserid`.

Produkt WebSphere MQ používá předponu `ibmwebspheremq` na štítku, aby se předešlo 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 v případě, že je konec kanálu, který se chová jako server SSL nebo TLS, definován buď s parametrem SSLCAUTH nastaveným na hodnotu REQUIRED, nebo s hodnotou parametru SSLPEER. Další informace o anonymnímu připojení správce front najdete v tématu “Anonymní připojení klienta ke správci front” na stránce 212.

Použití certifikátů podepsaných sebou samým pro vzájemné ověření klienta a správce front

Chcete-li implementovat vzájemné ověření mezi klientem a správcem front pomocí podepsaných certifikátů SSL nebo TLS, postupujte podle těchto ukázkových instrukcí.

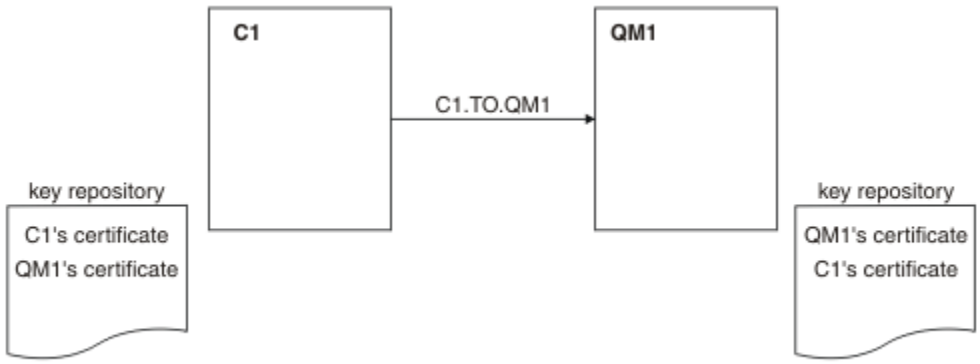
Informace o této úloze

Scénář:

- Máte klienta, C1, a správce front QM1, který musí komunikovat zabezpečeně. Požadujete vzájemnou autentizaci, která bude provedena mezi C1 a QM1.
- Rozhodli jste se otestovat zabezpečenou komunikaci pomocí certifikátů podepsaných sebou samým.

Produkt DCM v systému IBM i nepodporuje certifikáty s automatickým podpisem, takže tato úloha není použitelná na systémech IBM i .

Výsledná konfigurace vypadá takto:



Obrázek 23. Konfigurace vyplývající z této úlohy

V produktu Obrázek 17 na stránce 209obsahuje úložiště klíčů pro QM1 certifikát pro QM1 a veřejný certifikát z C1. Úložiště klíčů pro C1 obsahuje certifikát pro C1 a veřejný certifikát z QM1.

Postup

1. Připravte úložiště klíčů na klientu a správci front podle operačního systému:
   - Na systémech UNIX, Linuxa Windows.
2. Vytvořte certifikáty podepsané sebou samým pro klienta a správce front:
   - Na systémech UNIX, Linuxa Windows.
3. Extrahuje kopii každého certifikátu:
   - Na systémech UNIX, Linuxa Windows.
4. Přeneste veřejnou část certifikátu C1 na systém QM1 a naopak s použitím obslužného programu, jako je FTP.
5. Přidejte certifikát partnera do úložiště klíčů pro klienta a správce front:
   - Na systémech UNIX, Linuxa Windows.
6. Zadejte příkaz REFRESH SECURITY TYPE (SSL) ve správci front.
7. Definujte kanál připojení klienta jedním z následujících způsobů:
   - Použití volání MQCONNX se strukturou MQSCO na C1, jak je popsáno v tématu Vytvoření kanálu připojení klienta na klientovi WebSphere MQ MQI.
   - Pomocí tabulky definic kanálů klienta, jak je popsáno v tématu Vytvoření připojení serveru a definic připojení klienta na serveru .
8. V systému QM1definujte kanál připojení serveru vyvoláním příkazu, jako je tento příklad:

```
DEFINE CHANNEL(C1.TO.QM1) CHLTYPE(SVRCONN) TRPTYPE(TCP) SSLCIPH(RC4_MD5_US)
SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL from C1 to QM1')
```

Kanál musí mít stejný název jako kanál připojení klienta, který jste definovali v kroku 6, a použít stejnou položku CipherSpec.

Výsledky

Klíčová úložiště a kanály se vytvářejí podle ilustrace v části Obrázek 17 na stránce 209 .

Jak pokračovat dále

Zkontrolujte, zda byla úloha úspěšně dokončena pomocí příkazů DISPLAY. Pokud byla úloha úspěšná, výsledný výstup je podobný výsledku, který je zobrazen v následujícím příkladu.

Ve správci front QM1zadejte následující příkaz:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
```

Výsledný výstup je podobný následujícímu příkladu:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(C1.TO.QM1)                      CHLTYPE(SVRCONN)
   CONNAME(9.20.35.92)                       CURRENT
   SSLCERTI("CN=QM1,OU=WebSphere MQ Development,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5E:02,CN=QM2,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                           SUBSTATE(RECEIVE)
```

Je volitelné nastavit atribut filtru SSLPEER pro definice kanálu. Je-li nastavena definice kanálu SSLPEER, musí se její hodnota shodovat s DN subjektu v certifikátu partnera, který byl vytvořen v kroku 2. Po úspěšném připojení zobrazí pole SSLPEER ve výstupu DISPLAY CHSTATUS rozlišující název DN certifikátu vzdáleného klienta.

Použití certifikátů podepsaných CA pro vzájemné ověření klienta a správce front

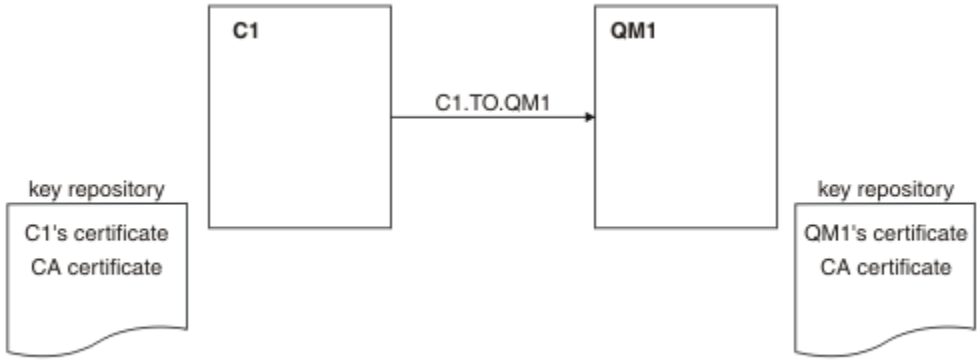
Chcete-li implementovat vzájemné ověření mezi klientem a správcem front pomocí certifikátů SSL nebo TLS, postupujte podle těchto ukázkových instrukcí.

Informace o této úloze

Scénář:

- Máte klienta, C1, a správce front QM1, který musí komunikovat zabezpečeně. Požadujete vzájemnou autentizaci, která bude provedena mezi C1 a QM1.
- V budoucnu se chystáte použít tuto síť v provozním prostředí, a proto jste se rozhodli používat certifikáty podepsané CA od začátku.

Výsledná konfigurace vypadá takto:



Obrázek 24. Konfigurace vyplývající z této úlohy

V produktu Obrázek 18 na stránce 210obsahuje úložiště klíčů pro C1 certifikát pro C1 a certifikát CA. Úložiště klíčů pro QM1 obsahuje certifikát pro QM1 a certifikát CA. V tomto příkladu byl certifikát C1i certifikát QM1vydáván stejným CA. Pokud byl certifikát C1a certifikát QM1vydáván různými CA, pak musí úložiště klíčů C1 a QM1 obsahovat obě certifikáty CA.

Postup

1. Připravte úložiště klíčů na klientu a správci front podle operačního systému:
   - Na systémech UNIX, Linuxa Windows.
2. Vyžádejte si certifikát podepsaný CA pro klienta a správce front.

   Pro klienta a správce front můžete použít různé CA.
   - Na systémech UNIX, Linuxa Windows.
3. Přidejte certifikát vydavatele certifikátů do úložiště klíčů pro klienta a správce front.

   Pokud klient a správce front používají různé certifikační autority, musí být certifikát CA pro každou certifikační autoritu přidán do obou úložišť klíčů.
   - Na systémech UNIX, Linuxa Windows.
4. Přidejte certifikát podepsaný CA do úložiště klíčů pro klienta a správce front:
   - Na systémech UNIX, Linuxa Windows.
5. Definujte kanál připojení klienta jedním z následujících způsobů:
   - Použití volání MQCONNX se strukturou MQSCO na C1, jak je popsáno v tématu Vytvoření kanálu připojení klienta na klientovi WebSphere MQ MQI.
   - Pomocí tabulky definic kanálů klienta, jak je popsáno v tématu Vytvoření připojení serveru a definic připojení klienta na serveru .
6. V systému QM1definujte kanál připojení serveru vyvoláním příkazu, jako je tento příklad:

   ```
   DEFINE CHANNEL(C1.TO.QM1) CHLTYPE(SVRCONN) TRPTYPE(TCP) SSLCIPH(RC2_MD5_EXPORT)
   SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL from C1 to QM1')
   ```

   Kanál musí mít stejný název jako kanál připojení klienta, který jste definovali v kroku 6, a použít stejnou položku CipherSpec.

Výsledky

Klíčová úložiště a kanály se vytvářejí tak, jak je znázorněno v části Obrázek 18 na stránce 210.

Jak pokračovat dále

Zkontrolujte, zda byla úloha úspěšně dokončena pomocí příkazů DISPLAY. Pokud byla úloha úspěšná, výsledný výstup je podobný tomu, který je zobrazen v následujícím příkladu.

Ve správci front QM1zadejte následující příkaz:

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
```

Výsledný výstup je podobný následujícímu příkladu:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(C1.TO.QM1)                      CHLTYPE(SVRCONN)
   CONNAME(9.20.35.92)                     CURRENT
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMA,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
```

Pole SSLPEER ve výstupu DISPLAY CHSTATUS obsahuje DN subjektu certifikátu vzdáleného klienta, který byl vytvořen v kroku 2. Název vydavatele se shoduje s DN subjektu certifikátu CA, který podepsal osobní certifikát přidaný v kroku 4.

Anonymní připojení klienta ke správci front

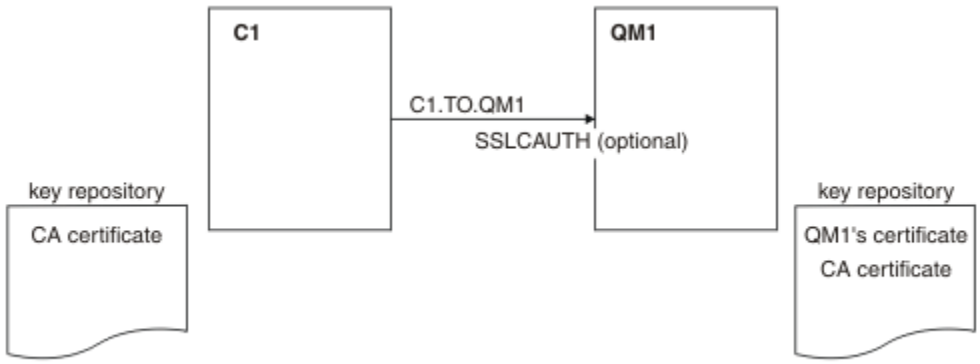
Chcete-li upravit systém se vzájemným ověřováním a umožnit anonymnímu připojení správce front k jinému správci front, postupujte podle těchto ukázkových pokynů.

Informace o této úloze

Scénář:

- Váš správce front a klient (QM1 a C1) byli nastavi jako v produktu “Použití certifikátů podepsaných CA pro vzájemné ověření klienta a správce front” na stránce 210.
- Chcete změnit C1 tak, aby se připojoval anonymně k QM1.

Výsledná konfigurace vypadá takto:



Obrázek 25. Klient a správce front umožňující anonymní připojení

Postup

1. Odeberte osobní certifikát z úložiště klíčů pro C1podle operačního systému:
   - Na systémech UNIX, Linuxa Windows. Certifikát je označen takto:

– `ibmwebspheremq` následováno vaším ID uživatele pro přihlášení složené do malých písmen, například `ibmwebspheremqmyuserid`.

2. Restartujte aplikaci klienta nebo ukončete aplikaci klienta a znovu otevřete všechna připojení SSL nebo TLS.
3. Povolit anonymní připojení ve správci front zadáním následujícího příkazu:

```
ALTER CHANNEL(C1.TO.QM1) CHLTYPE(SVRCONN) SSLCAUTH(OPTIONAL)
```

Výsledky

Klíčová úložiště a kanály se mění podle ilustrace v části Obrázek 19 na stránce 212

Jak pokračovat dále

Na konci kanálu je přítomnost hodnoty parametru názvu partnera na obrazovce stavu kanálu indikuje, že došlo k přetečení certifikátu klienta.

Zadáním některých příkazů DISPLAY ověřte, zda byla úloha úspěšně dokončena. Pokud byla úloha úspěšná, výsledný výstup je podobný jako v následujícím příkladu:

Ve správci front QM1zadejte následující příkaz:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
```

Výsledný výstup bude vypadat podobně jako v následujícím příkladu:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(C1.TO.QM1)                      CHLTYPE(SVRCONN)
   CONNAME(9.20.35.92)                     CURRENT
   SSLCERTI( )                             SSLPEER( )
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
```

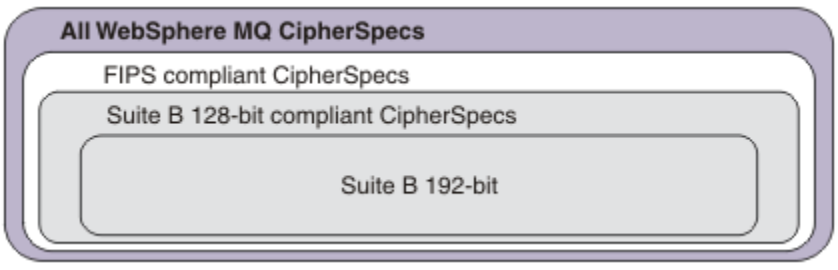
Pole SSLCERTI a SSLPELER jsou prázdná, což ukazuje, že C1 neodeslal certifikát.

Určení CipherSpecs

Zadejte CipherSpec pomocí parametru **SSLCIPH** buď v příkazu **DEFINE CHANNEL** MQSC, nebo v příkazu **ALTER CHANNEL** MQSC.

Některé ze specifikací CipherSpecs , které můžete použít s produktem IBM WebSphere MQ , vyhovují standardu FIPS. Jiné, například `NULL_MD5`, nejsou. Podobně některé specifikace CipherSpecs odpovídající standardu FIPS jsou také kompatibilní se standardem Suite B, i když jiné kompatibilní 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:



Specifikace šifer, které můžete použít s podporou zabezpečení SSL a TLS systému IBM WebSphere MQ , jsou uvedeny v následující tabulce. Požadujete-li osobní certifikát, určíte velikost klíče pro dvojici veřejný

a soukromý klíč. Velikost klíče, která se používá během navázání komunikace SSL, je velikost uložená v certifikátu, pokud není určena CipherSpec, jak je uvedeno v tabulce.

Název specifikace šifrování	Použitý protokol	Algoritmus MAC	Šifrovací algoritmus	Šifrování bitů	FIPS[1]	Sada B 128 bitů	Sada B 192 bitů
NULL_MD5 [a]	SSL 3.0	MD5	Není	0	Ne	Ne	Ne
NULL_SHA [a]	SSL 3.0	SHA-1	Není	0	Ne	Ne	Ne
RC4_MD5_EXPORT [2] [a]	SSL 3.0	MD5	RC4	40	Ne	Ne	Ne
RC4_MD5_US [a]	SSL 3.0	MD5	RC4	128	Ne	Ne	Ne
RC4_SHA_US [a]	SSL 3.0	SHA-1	RC4	128	Ne	Ne	Ne
RC2_MD5_EXPORT [2] [a]	SSL 3.0	MD5	RC2	40	Ne	Ne	Ne
DES_SHA_EXPORT [2] [a]	SSL 3.0	SHA-1	DES	56	Ne	Ne	Ne
RC4_56_SHA_EXPORT1024 [3] [b]	SSL 3.0	SHA-1	RC4	56	Ne	Ne	Ne
DES_SHA_EXPORT1024 [3] [b]	SSL 3.0	SHA-1	DES	56	Ne	Ne	Ne
TLS_RSA_WITH_AES_128_CBC_SHA [a]	TLS 1.0	SHA-1	AES	128	Ano	Ne	Ne
TLS_RSA_WITH_AES_256_CBC_SHA [4] [a]	TLS 1.0	SHA-1	AES	256	Ano	Ne	Ne
TLS_RSA_WITH_DES_CBC_SHA [a]	TLS 1.0	SHA-1	DES	56	Č.[5]	Ne	Ne
FIPS_WITH_DES_CBC_SHA [b]	SSL 3.0	SHA-1	DES	56	Č.[6]	Ne	Ne
TLS_RSA_WITH_AES_128_GCM_SHA256 [b]	TLS 1.2	AEAD AES-128 GCM	AES	128	Ano	Ne	Ne
TLS_RSA_WITH_AES_256_GCM_SHA384 [b]	TLS 1.2	AEAD AES-256 GCM	AES	256	Ano	Ne	Ne
TLS_RSA_WITH_AES_128_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES	128	Ano	Ne	Ne
TLS_RSA_WITH_AES_256_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES	256	Ano	Ne	Ne
ECDHE_ECDSA_RC4_128_SHA256 [b]	TLS 1.2	SHA-1	RC4	128	Ne	Ne	Ne
ECDHE_RSA_RC4_128_SHA256 [b]	TLS 1.2	SHA_1	RC4	128	Ne	Ne	Ne
ECDHE_ECDSA_AES_128_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES	128	Ano	Ne	Ne
ECDHE_ECDSA_AES_256_CBC_SHA384 [b]	TLS 1.2	SHA-384	AES	256	Ano	Ne	Ne
ECDHE_RSA_AES_128_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES	128	Ano	Ne	Ne
ECDHE_RSA_AES_256_CBC_SHA384 [b]	TLS 1.2	SHA-384	AES	256	Ano	Ne	Ne
ECDHE_ECDSA_AES_128_GCM_SHA256 [b]	TLS 1.2	AEAD AES-128 GCM	AES	128	Ano	Ano	Ne
ECDHE_ECDSA_AES_256_GCM_SHA384 [b]	TLS 1.2	AEAD AES-256 GCM	AES	256	Ano	Ne	Ano

Název specifikace šifrování	Použitý protokol	Algoritmus MAC	Šifrovací algoritmus	Šifrování bitů	FIPS[1]	Sada B 128 bitů	Sada B 192 bitů
ECDHE_RSA_AES_128_GCM_SHA256 [b]	TLS 1.2	AEAD AES-128 GCM	AES	128	Ano	Ne	Ne
ECDHE_RSA_AES_256_GCM_SHA384 [b]	TLS 1.2	AEAD AES-256 GCM	AES	256	Ano	Ne	Ne
TLS_RSA_WITH_NULL_SHA256 [b]	TLS 1.2	SHA-256	Není	0	Ne	Ne	Ne
ECDHE_RSA_NULL_SHA256 [b]	TLS 1.2	SHA-1	Není	0	Ne	Ne	Ne
ECDHE_ECDSA_NULL_SHA256 [b]	TLS 1.2	SHA-1	Není	0	Ne	Ne	Ne
TLS_RSA_WITH_NULL_NULL [b]	TLS 1.2	Není	Není	0	Ne	Ne	Ne
TLS_RSA_WITH_RC4_128_SHA256 [b]	TLS 1.2	SHA-1	RC4	128	Ne	Ne	Ne

Notes:

1. Uvádí, zda má specifikace šifrování certifikaci FIPS na platformě s certifikací FIPS. Vysvětlení FIPS viz Federal Information Processing Standards (FIPS).
2. 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.
3. Velikost klíče pro navázání komunikace je 1024 bitů.
4. Tuto CipherSpec nelze použít k zabezpečení připojení z produktu WebSphere MQ Explorer ke správci front, pokud nejsou pro prostředí JRE používané průzkumníkem použity příslušné neomezené soubory zásad.
5. Tato specifikace šifrování byla certifikována FIPS 140-2 před 19. květnem 2007.
6. 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.
7. Tuto specifikaci CipherSpec lze použít k přenosu až 32 GB dat, než bude připojení ukončeno chybou AMQ9288. Chcete-li se vyhnout této chybě, při použití této specifikace šifrování nepoužívejte buď algoritmus tripple DES, nebo povolte reset tajného klíče.

Podpora platformy:

- a K dispozici na všech podporovaných platformách.
- b K dispozici pouze na platformách UNIX, Linux, and Windows .

Související pojmy

“Digitální certifikáty a kompatibilita CipherSpec v produktu IBM WebSphere MQ” na stránce 34
Toto téma poskytuje informace o tom, jak vybrat příslušné CipherSpecs a digitální certifikáty pro svou strategii zabezpečení, a to tak, že nastiňují vztah mezi CipherSpecs a digitálními certifikáty v produktu IBM WebSphere MQ.

Související odkazy

Definovat kanál
POZMĚNIT KANÁL

Získání informací o CipherSpecs pomocí produktu IBM WebSphere MQ Explorer

Produkt IBM WebSphere MQ Explorer můžete použít k zobrazení popisů specifikace CipherSpecs.

Chcete-li získat informace o CipherSpecs v produktu “Určení CipherSpecs” na stránce 213, postupujte takto:

1. Otevřete produkt **IBM WebSphere 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.

Alternativy ke specifikaci CipherSpecs

Na těchto platformách, kde operační systém poskytuje podporu zabezpečení SSL, může váš systém podporovat nové specifikace CipherSpecs. Můžete uvést novou CipherSpec s parametrem SSLCIPH, ale hodnota, kterou zadáte, závisí na použité platformě.

Poznámka: Tento oddíl se nevztahuje na systémy UNIX, Linux nebo Windows , protože CipherSpecs jsou dodávány s produktem WebSphere MQ , takže nové CipherSpecs nebudou po odeslání k dispozici.

Na těchto platformách, kde operační systém poskytuje podporu zabezpečení SSL, může váš systém podporovat nové specifikace CipherSpecs , které nejsou zahrnuty v produktu “Určení CipherSpecs” na stránce 213. Můžete uvést novou CipherSpec s parametrem SSLCIPH, ale hodnota, kterou zadáte, závisí na použité platformě. Ve všech případech musí specifikace *odpovídat* odpovídat specifikaci SSL CipherSpec , která je platná a podporovaná verzí protokolu SSL, který systém běží.

IBM i

Dvouznakový řetězec reprezentující hexadecimální hodnotu.

Další informace o povolených hodnotách naleznete v příslušné dokumentaci k produktu (vyhledejte řetězec *cipher_spec* v dokumentaci k produktu IBM i).

Pro uvedení hodnoty můžete použít buď příkaz CHGMQMCHL nebo CRTMQMCHL, například:

```
CRTMQMCHL CHLNAME('channel name') SSLCIPH('hexadecimal value')
```

Chcete-li nastavit parametr SSLCIPH , můžete také použít příkaz ALTER QMGR MQSC.

z/OS

Dvouznakový řetězec reprezentující hexadecimální hodnotu. Hexadecimální kódy odpovídají hodnotám definovaným v protokolu SSL.

Další informace naleznete v popisu rozhraní gsk_environment_open () v kapitole odkazů rozhraní API systému *z/OS Cryptographic Services System SSL Programming*, SC24-5901, kde je uveden seznam všech podporovaných specifikací šifer SSL V3.0 a TLS V1.0 ve formátu dvouciferných hexadecimálních kódů.

Pokyny pro klastry WebSphere MQ

Při použití klastrů WebSphere MQ je nejbezpečnější použít názvy CipherSpec v produktu “Určení CipherSpecs” na stránce 213. Používáte-li alternativní specifikaci, uvědomte si, že specifikace nemusí být platná na jiných platformách. Další informace jsou uvedeny v tématu “SSL a klastry” na stránce 243.

Určení položky CipherSpec pro klienta IBM WebSphere MQ MQI

Existují tři možnosti zadání volby CipherSpec pro klienta IBM WebSphere MQ MQI.

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 třídami IBM WebSphere MQ pro třídy Java a IBM WebSphere MQ pro platformu JMS

Třídy IBM WebSphere MQ pro třídy Java a IBM WebSphere MQ pro platformu JMS specifikují CipherSuites jinak než u jiných platforem.

Informace o určení sady CipherSuite s třídami IBM WebSphere MQ pro jazyk Java naleznete v tématu Podpora zabezpečení SSL (Secure Sockets Layer).

Informace o určení sady CipherSuite s třídami produktu IBM WebSphere MQ pro platformu JMS naleznete v tématu Použití zabezpečení SSL (Secure Sockets Layer) s třídami produktu WebSphere MQ pro službu JMS.

Auditování

Můžete zkontrolovat narušení zabezpečení nebo pokusy o narušení pomocí zpráv událostí. Zabezpečení vašeho systému můžete také zkontrolovat pomocí IBM WebSphere 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 zabezpečení SSL pro klastry vezměte v úvahu některé další pokyny.

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 s použitím nástroje RACF v systému z/OSnebo OAM na jiných platformách.

Informace o této úloze

Pomocí systémových prostředků zabezpečení platformy a mechanismu řízení přístupu v produktu WebSphere MQ můžete řídit přístup k frontám.

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 produktu WebSphere MQ pro systém 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 může kontrola zahrnovat buď ID uživatele přijaté ze sítě, nebo které bylo odvozeno od uživatele MCAUSER, nebo z obou. Tuto volbu použijte, je-li odkaz důvěryhodný a ověřený.

   ONLYMCA (pouzez/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 (pouzez/OS)
   Co se týče CTX, ale žádné ID uživatele přijaté ze sítě se nepoužije.

Autorizace vkládání zpráv ve vzdálených frontách klastru

Na své platformě autorizujte přístup pro připojení ke správci front a umístěte jej do fronty na tohoto správce 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 systémy UNIX, Linux a Windows zadejte následující příkazy:

```
setmqaut -m QMgrName -t qmgr -g GroupName +connect
setmqaut -m QMgrName -t queue -n QueueName -g GroupName -all +put
```

Uživatel může vkládat zprávy pouze do určené fronty klastru a žádné další fronty klastru.

Názvy proměnných mají následující význam:

QMgrName
Název správce 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 188.

Související informace
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 blokovat připojení kanálu klastru založené na: vzdálené adrese IP, názvu vzdáleného správce front nebo rozlišujícím názvu SSL/TLS poskytovaného 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.

   systémy Windows, UNIX and Linux

   - 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.

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)
   ```

Výsledky

Správce front, který je vynucený, se nemění: jeho lokální definice klastru ukazují, že se nachází 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.

SSL a klastry

Při konfiguraci zabezpečení SSL pro klastry mějte na paměti, že definice kanálu CLUSRCVR je rozšířena na další správce front jako automaticky definovaný kanál CLUSSDR. Pokud kanál CLUSRCVR používá zabezpečení SSL, musíte nakonfigurovat zabezpečení SSL na všech správcích front, které komunikují prostřednictvím kanálu.

Další informace o zabezpečení SSL najdete v tématu Podpora produktuWebSphere MQ pro zabezpečení SSL a TLS. Doporučení je obecně použitelné pro kanály klastru, ale možná byste měli věnovat zvláštní pozornost následujícím:

V klastru IBM WebSphere 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 produkt CLUSRCVR nakonfigurován pro připojení SSL, platí následující pokyny:

- Všichni správci front, kteří chtějí komunikovat s touto CLUSRCVR , musí mít přístup k podpoře SSL. Toto ustanovení SSL 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 WebSphere 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=WebSphere 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 v systémech UNIX, Linux nebo 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 SSL 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 RC4_MD5_US).

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 zabezpečení SSL

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 specifikace CipherSpecs mohou být nové v aktuálním vydání produktu WebSphere MQ a nejsou ve starších verzích podporovány. 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.

Proveďte upgrade všech správců front v klastru na produkt WebSphere MQ V6 nebo vyšší, pokud tyto úrovně ještě nejsou na těchto úrovních. Distribuujte certifikáty a klíče tak, aby SSL fungovalo z každého z nich.

Informace o této úloze

Změňte jeden CLUSRCVR najednou a umožněte, aby se změny procházela klastrem, a teprve pak změňte další. Ujistěte se, že jste nezměnili opačnou cestu, dokud nejsou změny pro aktuální kanál distribuovány po celém klastru.

Postup

1. Přepněte kanály CLUSRCVR na zabezpečení SSL v libovolném pořadí, které chcete.

   Změny proudí v opačném směru přes kanály, které se nezměnily na SSL.
2. Přepněte všechny ruční kanály CLUSSDR na SSL.

   To však nemá žádný vliv na činnost klastru, pokud nepoužijete příkaz REFRESH CLUSTER s volbou REPOS(YES) .

   Poznámka: Použití příkazu **REFRESH CLUSTER** může narušit provoz velkých klastrů, a to jak při spuštění, tak později v 27denních intervalech, kdy objekty klastru automaticky rozesílají aktualizace stavu všem zainteresovaným správcům front. Viz téma Aktualizace velkých klastrů mohou ovlivnit jejich výkon a dostupnost.

Související pojmy

“Určení CipherSpecs” na stránce 213
Zadejte CipherSpec pomocí parametru **SSLCIPH** buď v příkazu **DEFINE CHANNEL** MQSC, nebo v příkazu **ALTER CHANNEL** MQSC.

“Digitální certifikáty a kompatibilita CipherSpec v produktu IBM WebSphere MQ” na stránce 34
Toto téma poskytuje informace o tom, jak vybrat příslušné CipherSpecs a digitální certifikáty pro svou strategii zabezpečení, a to tak, že nastiňují vztah mezi CipherSpecs a digitálními certifikáty v produktu IBM WebSphere MQ.

Související informace

Klastrování: Využití doporučených postupů pro příkaz REFRESH CLUSTER

Zakázání zabezpečení SSL nebo TLS v klastrovaných správcích front a kanálech

Chcete-li vypnout SSL nebo TLS, nastavte parametr SSLCIPH na ' '. 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 .

   Můžete vypnout SSL nebo TLS na přijímacích kanálech klastru v libovolném pořadí, které chcete.

   Všimněte si, že změny proudí směrem opačným směrem přes kanály, na kterých jste ponechal SSL nebo TLS aktivní.
2. Zkontrolujte, zda se nová hodnota odrazí ve všech ostatních správcích front, pomocí příkazu **DISPLAY CLUSQMGR(*)** ALL.
3. Vypněte SSL nebo TLS na všech manuálových kanálech odesílatele klastru.

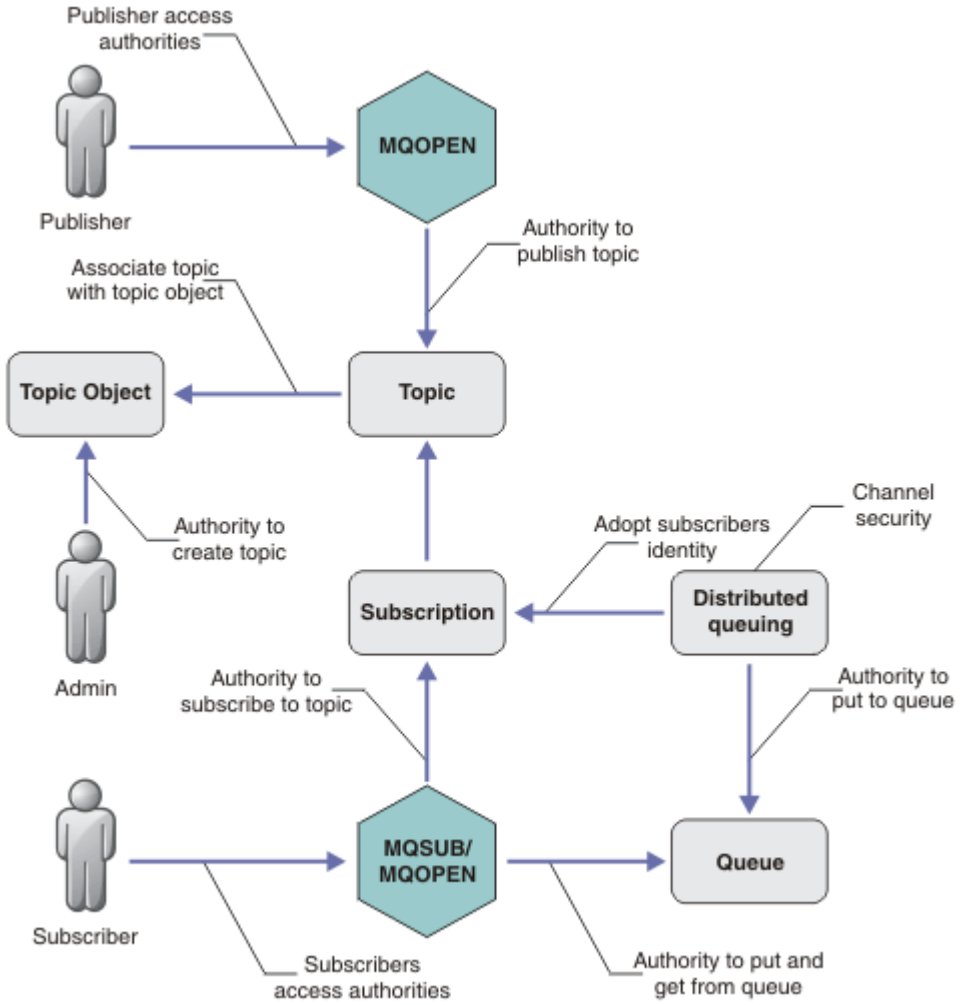
   To nemá žádný vliv na činnost klastru, pokud nepoužijete příkaz **REFRESH CLUSTER** s volbou REPOS (YES) .

   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 26 na stránce 246 a popsány v následujícím příkladu.



Obrázek 26. Vztahy zabezpečení typu publikování/odběr

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. “Model zabezpečení témat” na stránce 248 vysvětluje, jak zabezpečujete 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. Prohlédněte si příklady, “Udělit uživateli přístup k odběru tématu” na stránce 252 a “Udělit přístup uživateli k publikování v rámci tématu” na stránce 257.

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 249

Přihlásit se k odběru pomocí tématu

“Přihlášení k odběru pomocí řetězce tématu, ve kterém uzel tématu neexistuje” na stránce 250

Přihlásit se k odběru tématu se zástupnými znaky

“Přihlášení k odběru pomocí řetězce tématu, který obsahuje zástupné znaky” na stránce 250

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 262.

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 250.

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

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 WebSphere MQ jsou kanály konfigurovány s použitím PUTAUT=DEF umisťují zprávy do cílových front pomocí oprávnění procesu kanálu. Můžete upravit konfiguraci kanálu tak, aby používala příkaz PUTAUT=CTX tak, aby odebírající uživatel měl oprávnění šířit odběr do jiného správce front v klastru.

Téma Zabezpečení publikování/odběru mezi správci front 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. WebSphere MQ Administrator-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.

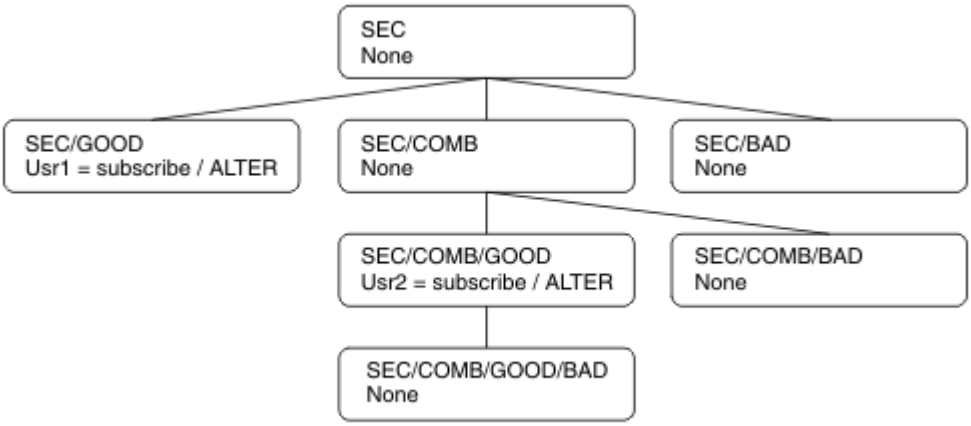
Atributy zabezpečení jsou seznam přístupových práv, který označuje, které oprávnění má určité ID uživatele operačního systému nebo skupiny zabezpečení k objektu tématu.

Prohlédněte si následující příklad, kde byly objekty tématu definovány s atributy zabezpečení, nebo s zobrazenými oprávněními:

Tabulka 17. Příklad oprávnění k objektu tématu

Název tématu	Řetězec tématu	Autority-ne z/OS	Oprávnění z/OS
SECROOT	SEC	Není	Není
SECGOOD	SEC/GOOD	usr1+subscribe	ALTER HLQ.SUBSCRIBE.SECGOOD
SECBAD	SEC/BAD	Není	Není HLQ.SUBSCRIBE.SECBAD
SECCOMB	SEC/COMB	Není	Není HLQ.SUBSCRIBE.SECCOMB
SECCOMBB	SEC/COMB/ GOOD/BAD	Není	Není HLQ.SUBSCRIBE.SECCOMBB
SECCOMBG	SEC/COMB/GOOD	usr2+subscribe	ALTER HLQ.SUBSCRIBE.SECCOMBG
SECCOMBN	SEC/COMB/BAD	Není	Není HLQ.SUBSCRIBE.SECCOMBN

Strom témat s přidruženými atributy zabezpečení na každém uzlu 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.

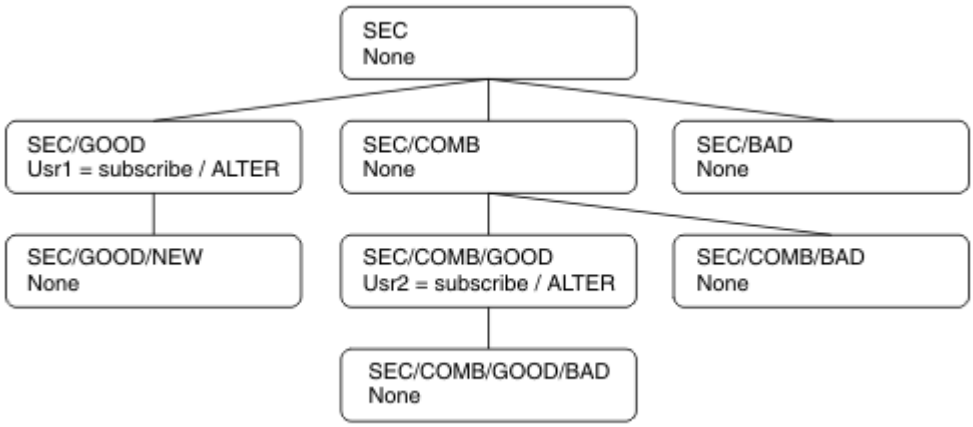
Přihlášení k odběru pomocí řetězce tématu, ve kterém uzel tématu existuje

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. When an alias queue resolves to another queue, checks are *ne* made on the underlying queue. 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 parametr **SUBUSER** , ovlivní způsob kontroly, jak ukazuje Tabulka 18 na stránce 252:

Tabulka 18. 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 administrátora
	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 nastavení řízení přístupu na témata způsobem, který umožňuje použití ovladače zabezpečení podle potřeby.

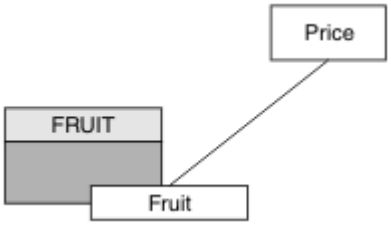
Udělit uživateli přístup k odběru tématu

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 27. Příklad přístupu k objektu tématu

Tabulka 19. 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:
   - 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:

     Windows Linux UNIX **systémy Windows, UNIX and Linux**

     ```
     setmqaut -t topic -n FRUIT -p USER1 +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:

- Windows Linux UNIX Na ostatních platformách 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.

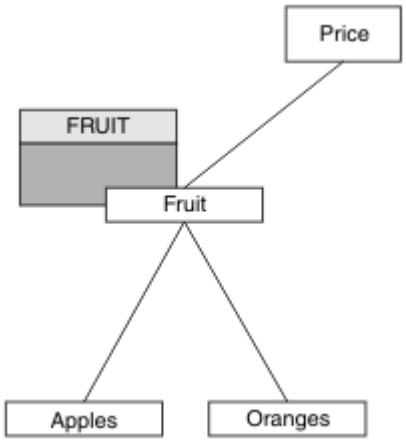
Toto téma je druhé v seznamu úloh, které vás informují o tom, jak udělit přístup k tématům více uživateli.

Než začnete

Toto téma používá nastavení popsané v části “Udělit uživateli přístup k odběru tématu” na stránce 252.

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 28. Příklad udělení přístupu k tématu ve stromu témat

Tabulka 20. 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 systému z/OS a k odběru přístupu k 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:

- Na konzole 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 v systému z/OS , jsou shodné s těmi, které jste obdrželi v předchozí úloze jako stejné objekty tématu a profily řídí 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.

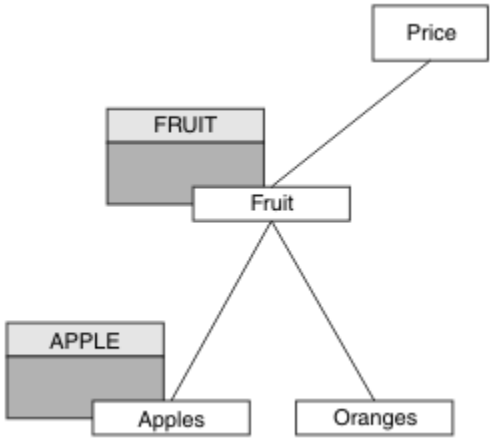
Toto téma je třetí ze seznamu úloh, které vám říkají, jak udělit přístup k odběru témat více než jedním uživatelem.

Než začnete

Toto téma používá nastavení popsané v části “Udělte uživateli přístup k odběru tématu hlouběji do stromu.” na stránce 253.

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 29. Udělení přístupu ke specifickým tématům v rámci stromu témat

Tabulka 21. 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:
   - 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:

systémy Windows, UNIX and Linux

```
setmqaut -t topic -n APPLE -p USER2 +sub
```

Výsledky

Pokud se v systému z/OS USER1 při pokusu 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. Pro první kontrolu se však vygeneruje zpráva RACF `ICH` :

```
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:

- 

Na platformách Windows, UNIX a Linux 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 na konzole z/OSobdržíte další zprávy produktu `ICH` na konzole. Tomuto se můžete vyhnout, pokud jste strom témat zabezpečili jiným způsobem.

Změnit řízení přístupu tak, aby se předešlo dalším zprávám

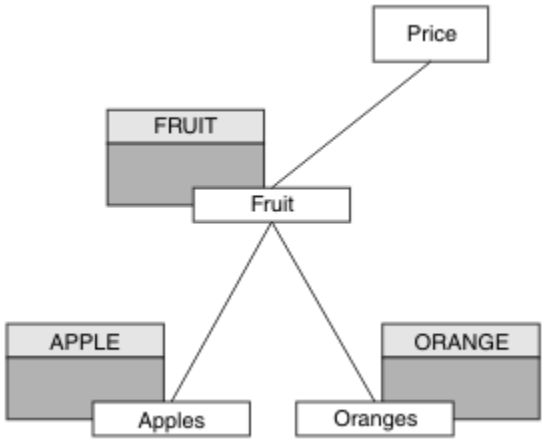
Toto téma je čtvrté v seznamu úloh, které vám sdělují, jak udělit přístup k odběru témat více uživateli a vyhnout se dalším zprávám RACF ICH408I na systému z/OS.

Než začnete

Toto téma vylepšuje nastavení popsané v části “Udělte jinému uživateli přístup k odběru pouze tématu hlouběji do stromu.” na stránce 255 tak, abyste se vyhnuli 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 30. 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:
   - Ostatní platformy:

     Nastavení ekvivalentního přístupu pomocí příkazů autorizace pro platformu:

     systémy Windows, UNIX and Linux

     ```
     setmqaut -t topic -n ORANGE -p USER1 +sub
     setmqaut -t topic -n APPLE -p USER1 +sub
     ```

Výsledky

V systému z/OS, když se produkt USER1 pokusí 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:

- 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"
```

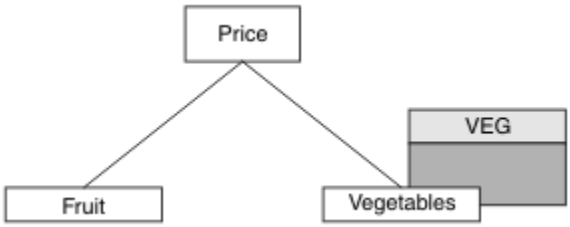
Udělit přístup uživateli k publikování v rámci tématu

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 31. Udělení přístupu pro publikování k tématu

Tabulka 22. 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:
   - 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:

     Windows Linux UNIX **systémy Windows, UNIX and Linux**

     ```
     setmqaut -t topic -n VEG -p USER1 +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:

- Windows Linux UNIX Na ostatních platformách 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.

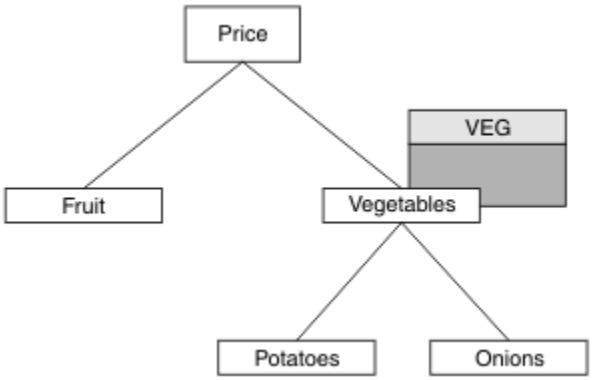
Toto téma je druhé v seznamu úloh, které vás informují o tom, jak udělit přístup k publikačním tématům více uživateli než jednomu uživateli.

Než začnete

Toto téma používá nastavení popsané v části “Udělit přístup uživateli k publikování v rámci tématu” na stránce 257.

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 32. Udělení přístupu pro publikování k tématu v rámci stromu témat

Tabulka 23. 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"` udělením přístupu k profilu produktu `hlq.PUBLISH.VEG` na systému z/OS nebo k publikování přístupu 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:

- Na konzole 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 v systému z/OS , jsou shodné s těmi, které jste obdrželi v předchozí úloze jako stejné objekty tématu a profily řídí 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

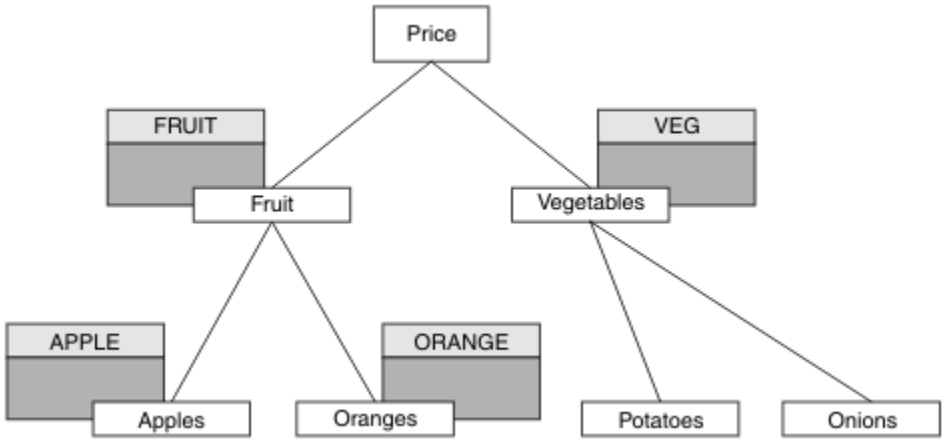
Toto téma je poslední v seznamu úloh, které vás informují o tom, jak udělit přístup k publikování a k odběru témat více než jedním uživatelem.

Než začnete

Toto téma používá nastavení popsané v části “Udělte uživateli přístup k tématu hlouběji do stromu.” na stránce 259.

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 33. Udělení přístupu pro publikování a odběr

Tabulka 24. 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

Tabulka 24. Příklad požadavků na publikování a přihlášení k odběru (pokračování)			
Téma	**Je vyžadován přístup pro**	**Požadovaný přístup pro publikování**	**Objekt tématu**
Cena/Ovoce/ Pomeranče	USER1		ORANŽOVÁ

Postup

Udělte přístup následujícím způsobem:

- 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:

  Windows Linux UNIX **systémy Windows, UNIX and Linux**

  ```
  setmqaut -t topic -n FRUIT -p USER1 +pub
  ```

Výsledky

V systému z/OS, když se produkt USER1 pokusí o publikování na téma `"Price/Fruit"` , kontrola zabezpečení volání MQOPEN se předá.

Když se příkaz USER2 pokusí o publikaci na téma `"Price/Fruit"` , výsledkem je selhání se zprávou `MQRC_NOT_AUTHORIZED` společně s:

- Windows Linux UNIX Na platformách Windows, UNIX a Linux následující 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 25. 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.

Tabulka 25. Úplný seznam přístupových oprávnění vedoucích k příkladům zabezpečení (pokračování)			
Téma	**Je vyžadován přístup pro**	**Požadovaný přístup pro publikování**	**Objekt tématu**
Cena/ Zelenina/ Potatony			
Cena/ Zelenina/ Onivy			

Pokud máte v rámci stromu témat různé požadavky na zabezpečení přístupu k zabezpečení na různých úrovních, pečlivé plánování zajistí, abyste v protokolu konzoly z/OS neobdrželi nadbytečná varování 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 26. 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.
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.

IBM WebSphere MQ Advanced Message Security

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

Přehled produktu IBM WebSphere MQ Advanced Message Security

Aplikace produktu IBM WebSphere MQ mohou používat produkt IBM WebSphere MQ 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

GSKit return codes used in IBM WebSphere MQ AMS messages

Chování, které se změnilo mezi verzí 7.0.1 a verzí 7.5

Protože se produkt IBM Advanced Message Security stal komponentou v produktu WebSphere MQ 7.5, došlo ke změně některých aspektů funkčnosti produktu IBM WebSphere MQ AMS , které mohou mít vliv na existující aplikace, administrativní skripty nebo procedury správy.

Před upgradem správců front na verzi 7.5si pečlivě prohlédněte následující seznam změn. Rozhodněte se, zda musíte naplánovat provedení změn existujících aplikací, skriptů a procedur před spuštěním migrace systémů na produkt IBM WebSphere MQ verze 7.5:

- Instalace produktu IBM WebSphere MQ AMS je součástí procesu instalace produktu WebSphere MQ .
- Schopnosti zabezpečení produktu IBM WebSphere MQ AMS jsou aktivovány s jeho instalací a řízeny zásadami zabezpečení. Chcete-li povolit, aby produkt IBM WebSphere MQ AMS zakročoval data, není třeba zachytávat zachytávače.
- Produkt IBM WebSphere MQ AMS v produktu WebSphere MQ verze 7.5 nevyžaduje použití příkazu **cfgmqs** jako v samostatné verzi produktu IBM WebSphere MQ AMS.

Vlastnosti a funkce produktu IBM WebSphere MQ Advanced Message Security

Produkt Advanced Message Security rozšiřuje služby zabezpečení produktu WebSphere 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 IBM WebSphere MQ AMS ověřuje, zda je odesilatel dat zpráv autorizován k vložení podepsaných zpráv do cílové fronty.

Zde je úplný seznam funkcí produktu IBM WebSphere MQ AMS :

- Zabezpečuje citlivé nebo vysoce hodnotové transakce zpracované produktem WebSphere 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 produkt WebSphere MQ.

Ošetření chyb

Advanced Message Security definuje frontu zpracování chyb ke správě 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 WebSphere MQ 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.

WebSphere MQ AMS používá SYSTEM.PROTECTION.ERROR.QUEUE jako frontu zpracování chyb. Všechny zprávy odeslané produktem IBM WebSphere MQ AMS do systému SYSTEM.PROTECTION.ERROR.QUEUE je předcházen záhlavím MQDLH.

Administrátor produktu WebSphere MQ může také definovat SYSTEM.PROTECTION.ERROR.QUEUE jako fronta aliasů odkazující na jinou frontu.

Klíčové pojmy

Seznamte se s klíčovými koncepty v produktu Advanced Message Security , abyste porozuměli tomu, jak nástroj funguje a jak efektivně spravovat.

Infrastruktura veřejných klíčů

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 přiřazeném 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

“Používání úložišť klíčů a certifikátů” na stránce 288
Chcete-li zajistit transparentní ochranu šifrování pro aplikace WebSphere MQ , produkt Advanced Message Security použije soubor úložiště klíčů, kde jsou uloženy certifikáty veřejných klíčů a soukromý klíč.

digitální certifikáty

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 aplikacích 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*.

Správce oprávnění k objektu

Produkt Object Authority Manager (OAM) je komponenta autorizační služby dodaná s produkty WebSphere MQ .

Přístup k entitám Advanced Message Security je řízen pomocí skupin uživatelů produktu WebSphere 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. 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

Podporovaná technologie

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 WebSphere MQ :

- Message Queue Interface (MQI)
- WebSphere MQ Java Message Service (JMS) 1.0.2 a 1.1.
- WebSphere MQ Základní třídy pro Java
- Třídy WebSphere MQ pro. Net v nespravovaném režimu

Poznámka: Produkt Advanced Message Security podporuje certifikační autority odpovídající standardu X.509 .

Známá omezení.

Informace o omezeních produktu IBM WebSphere MQ Advanced Message Security.

- Následující volby IBM WebSphere MQ nejsou podporovány:
  - Publikování/odběr.
  - Převod dat kanálu.
  - Distribuční seznamy.
  - Segmentace zpráv aplikace
  - Použití aplikací bez podprocesů využívajících uživatelskou proceduru rozhraní API na platformách HP-UX .
  - Třídy IBM WebSphere MQ pro .NET ve spravovaném režimu (připojení klienta nebo vazby).
  - Aplikace Message Service client for .NET (XMS).
  - Klient Message Service pro aplikace C/C++ (XMS supportPac IA94).
- Všechny aplikace Java jsou závislé na běhovém prostředí IBM Java .

Produkt IBM WebSphere MQ Advanced Message Security nepodporuje prostředí JRE poskytované jinými dodavateli.

- Klientské aplikace JMS a Java používající IBM WebSphere MQ Advanced Message Security v režimu klienta.

  Všechny služby JMS nebo Java, klientská aplikace (včetně agentů IBM WebSphere MQ Explorer a IBM WebSphere MQ Managed File Transfer) nemohou používat IBM WebSphere MQ Advanced Message Security v režimu klienta se správcem front WebSphere MQ starším než Version 7.5.

  Chcete-li používat zásady ochrany zpráv, tyto aplikace musí buď pracovat se správcem front produktu IBM WebSphere MQ Version 7.5 , nebo se připojit v režimu lokálních vazeb ke správci front ve stejném počítači jako aplikace.
- Měli byste se vyhnout umisťování dvou nebo více certifikátů se stejnými rozlišujícími názvy v jednom souboru úložiště klíčů, protože intereceptor produktu IBM WebSphere MQ Advanced Message Security s takovými certifikáty není definován.
- Adaptér prostředků IBM WebSphere MQ Version 7.5 nepodporuje produkt IBM WebSphere MQ Advanced Message Security. Pokud je vyžadována ochrana zpráv pro aplikace produktu IBM WebSphere MQ classes for JMS nebo IBM WebSphere MQ classes for Java spuštěné v prostředí aplikačního serveru, postupujte takto:
  - Aplikační server musí být konfigurován tak, aby používal adaptér prostředků produktu Version 8.0 nebo novější.
  - Je třeba použít také zachycení agenta MCA (Message Channel Agent).

Uživatelské scénáře

Seznamte se s možnými scénáři a seznamte se s obchodními cíli, které můžete dosáhnout pomocí produktu Advanced Message Security.

Stručná úvodní příručka pro platformy Windows

Pomocí této příručky můžete rychle nakonfigurovat produkt IBM Advanced Message Security , 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 WebSphere MQ pro systémy Windows .

Informace o použití příkazu **setmqenv** k inicializaci aktuálního prostředí tak, aby příslušné příkazy operačního systému WebSphere MQ mohly být umístěny a spuštěny operačním systémem, viz setmqenv.

1. Vytvoření správce front a fronty

Informace o této úloze

Všechny následující příklady používají frontu s názvem `TEST.Q` pro předávání zpráv mezi aplikacemi. Advanced Message Security pomocí zachytávačů podepisují a šifrují zprávy v místě, kam vstupují do infrastruktury WebSphere MQ prostřednictvím standardního rozhraní produktu WebSphere MQ . Základní nastavení se provádí v produktu WebSphere MQ a je konfigurováno v následujících krocích.

Průzkumník produktu WebSphere MQ můžete použít k vytvoření správce front QM_VERIFY_AMS a jeho lokální fronty s názvem `TEST.Q` tak, že použijete všechna výchozí nastavení průvodce, nebo můžete použít příkazy nalezené v `\WebSphere 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. Musíte 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
```

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 271.

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 Java pomocí vazeb klienta, musíte vytvořit úložiště klíčů a certifikáty JKS pomocí příkazu **keytool** , který je součástí prostředí JRE (další podrobnosti viz "Stručná úvodní příručka pro klienty Java" na stránce 278). Kroky v této příručce jsou správné pro všechny ostatní jazyky a pro aplikace Java používající lokální vazby.

Postup

1. Použijte grafické rozhraní IBM Key Management (`strmqikm.exe`) k vytvoření nové databáze klíčů pro uživatele `alice`.

   ```
   Type:       CMS
   Filename:   alicekey.kdb
   Location:   C:/Documents and Settings/alice/AMS
   ```

   Poznámka:

   - 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 vlastní podpis**; v tomto scénáři se používají certifikáty podepsané sebou samým.
4. Vytvořte certifikát identifikující uživatele `alice` pro použití v šifrování pomocí těchto polí:

   ```
   Key label: Alice_Cert
   Common Name: alice
   Organisation: IBM
   Country: GB
   ```

   Poznámka:

   - Pro účely této příručky používáme certifikát podepsaný 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 klíčové databáze a certifikáty located.This , musíte umístit zachytávače Advanced Message Security do adresáře, kde jsou klíčové databáze a certifikáty uloženy prostřednictvím souboru `keystore.conf` , který obsahuje tyto informace ve formě prostého textu. Každý uživatel musí mít samostatný soubor `keystore.conf` . 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" 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 (Cryptographic Message Syntax), JKS (Java Keystore) a JCEKS (Java Cryptographic Extension Keystore). Další informace jsou uvedeny v tématu “Struktura konfiguračního souboru úložiště klíčů (keystore.conf)” na stránce 288.
- *%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 “Používání úložišť klíčů a certifikátů” na stránce 288.
- 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/alice/AMS/bobkey.kdb" -pw passw0rd
   -label Bob_Cert -target bob_public.arm

   runmqakm -cert -add -db "C:/Documents and Settings/bob/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` , 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.

Stručná úvodní příručka pro platformy UNIX

Pomocí této příručky můžete rychle nakonfigurovat produkt IBM Advanced Message Security , aby poskytoval zabezpečení zpráv na platformách UNIX . 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.
- Sada IBM Global Security Kit
- MQ Advanced Message Security

Názvy komponent na každé specifické platformě naleznete v následujících tématech:

- Komponenty produktuIBM WebSphere MQ pro systémy Linux
- Komponenty produktuIBM WebSphere MQ pro systémy HP-UX

- Komponenty produktuIBM WebSphere MQ pro systémy AIX
- Komponenty produktuIBM WebSphere MQ pro systémy Solaris

1. Vytvoření správce front a fronty

Informace o této úloze

Všechny následující příklady používají frontu s názvem TEST.Q pro předávání zpráv mezi aplikacemi. Advanced Message Security pomocí zachytávačů podepisují a šifrují zprávy v místě, kam vstupují do infrastruktury WebSphere MQ prostřednictvím standardního rozhraní produktu WebSphere MQ . Základní nastavení se provádí v produktu WebSphere MQ a je konfigurováno v následujících krocích.

Průzkumník produktu WebSphere MQ můžete použít k vytvoření správce front QM_VERIFY_AMS a jeho lokální fronty s názvem TEST.Q tak, že použijete všechna výchozí nastavení průvodce, nebo můžete použít příkazy nalezené v <MQ_INSTALL_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. Musíte 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
```

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 277.

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 Java pomocí vazeb klienta, musíte vytvořit úložiště klíčů a certifikáty JKS pomocí příkazu **`keytool`** , který je součástí prostředí JRE (další podrobnosti viz “Stručná úvodní příručka pro klienty Java” na stránce 278). 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 do adresáře zachytávat zachytávače produktu 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` (Cryptographic Message Syntax), `JKS` (Java Keystore) a `JCEKS` (Java Cryptographic Extension Keystore). Další informace jsou uvedeny v tématu “Struktura konfiguračního souboru úložiště klíčů (keystore.conf)” na stránce 288.
- `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 “Používání úložišť klíčů a certifikátů” na stránce 288.

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` , 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.

Stručná úvodní příručka pro klienty Java

Tato příručka slouží k rychlé konfiguraci produktu IBM Advanced Message Security k zajištění zabezpečení zpráv pro aplikace v jazyce Java, které se připojují s použitím vazeb klienta. Po dokončení této operace jste vytvořili úložiště klíčů k ověření identit uživatelů a definované zásady podepisování a šifrování pro správce front.

Než začnete

Ujistěte se, že máte nainstalované příslušné komponenty, jak je popsáno v **Stručná úvodní příručka** (Windows nebo UNIX).

1. Vytvoření správce front a fronty

Informace o této úloze

Všechny následující příklady používají frontu s názvem `TEST.Q` pro předávání zpráv mezi aplikacemi. Advanced Message Security pomocí zachytávačů podepisují a šifrují zprávy v místě, kam vstupují do infrastruktury WebSphere MQ prostřednictvím standardního rozhraní produktu WebSphere MQ . Základní nastavení se provádí v produktu WebSphere 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, 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

Existují dva uživatelé, kteří se objevují v našem 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, 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 podle popisu v **Stručné úvodní příručce** (Windows nebo UNIX) 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
```

3. Musíte 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
```

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 282.

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 jazyce Java, které se připojují pomocí vazeb klienta. Plánujete-li používat aplikace Java pomocí 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 UNIX).

Postup

1. Vytvořte adresář, do kterého chcete vytvořit úložiště klíčů, například `/home/alice/.mqs`. Možná si ji budete přát vytvořit ve stejném adresáři, jaký používá **Stručná úvodní příručka** (Windows nebo UNIX) pro vaši platformu.

   Poznámka: Tento adresář bude 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 UNIX zkontrolujte, 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 do adresáře zachytávat zachytávače produktu 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 bude 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 bude 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 `keystore.conf` , protože jste následovali **Stručná úvodní příručka** (Windows nebo UNIX), můžete upravit existující, která se má přidat do výše uvedených řádků.
- Další informace viz “Struktura konfiguračního souboru úložiště klíčů (keystore.conf)” na stránce 288.

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. Například nástroj IBM GSKit Keyman (ikeyman) rozlišuje, že jste *extrahovat* 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 WebSphere 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
```

Než začnete

Ujistěte se, že verze jazyka Java, kterou používáte, má nainstalované neomezené soubory zásad JCE.

Poznámka: Verze jazyka Java dodaná v instalaci produktu WebSphere 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 UNIX) pro vaši platformu.

Postup

1. Chcete-li spustit tyto ukázkové aplikace JMS, použijte nastavení CLASSPATH pro vaši platformu, jak je zobrazeno v tématu Proměnné prostředí používané třídami produktu IBM WebSphere MQ pro platformu JMS , abyste zajistili, že bude 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

Chcete-li plně chránit připojení vzdálených front, musí být stejná zásada nastavena 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 v souladu s sadou zásad pro vzdálenou frontu. Například pro zásadu šifrování je zpráva zašifrována před tím, než je předána do produktu WebSphere MQ za účelem zpracování. Poté, co produkt Advanced Message Security zpracoval zprávu do vzdálené fronty, produkt WebSphere MQ ji umístí do přidružené přenosové fronty a předá ji cílovému správci front a cílové frontě.

Když se provede operace GET na 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 provedení Advanced Message Security , odeberte příznak tolerance.

Související odkazy

setmqspl (nastavit zásady zabezpečení)

Směrování chráněných zpráv pomocí produktu WebSphere Message Broker

IBM Advanced Message Security může chránit zprávy v infrastruktuře, kde je nainstalován produkt WebSphere Message Broker verze 8.0.0.1 (nebo novější). Před použitím zabezpečení v prostředí WebSphere Message Broker 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 produkt WebSphere Message Broker můžete buď povolit produktu WebSphere Message Broker zpracovat zprávy, aniž byste znali jejich obsah (Scénář 1), nebo aby byl autorizovaným uživatelem schopným přijímat a odesílat zprávy (Scénář 2).

Scénář 1-Zprostředkovatel zpráv nemůže vidět obsah zprávy

Než začnete

Měli byste mít svého zprostředkovatele zpráv WebSphere připojený k existujícímu 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 `route`Toje zpráva směrována buď na *bob*'s (`QBOB`),[1](`QCECIL`) nebo výchozí fronty (`QDEF`). Směrování je možné, protože produkt Advanced Message Security chrání pouze informační obsah zprávy a nikoli jeho záhlaví a vlastnosti, které zůstávají nechráněné a které lze číst prostřednictvím zprostředkovatele zpráv WebSphere Message Broker. Advanced Message Security je používán pouze *alice*, *bob* a *cecil*. Není nutné ji instalovat nebo konfigurovat pro produkt WebSphere Message Broker.

WebSphere Message Broker přijímá chráněnou zprávu z nezabezpečené fronty aliasů, aby se vyhnul 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 produktem WebSphere Message Broker a doručena do cílové fronty beze změn. Proto je stále podepsán původním autorem (oba *bob* a *cecil* přijímají pouze zprávy odeslané *alice*) a jsou chráněny jako předtím (mohou jej číst pouze *bob* a *cecil*). WebSphere Message Broker vloží přesměrovanou zprávu do nechráněného aliasu. Příjemci načtou zprávu z chráněné výstupní fronty, kde produkt IBM WebSphere MQ AMS transparentně dešifruje tuto zprávu.

Postup

1. Nakonfigurujte *alice*, *bob* a *cecil* pro použití produktu Advanced Message Security , jak je popsáno v příručce **Quick Start Guide** (Windows nebo UNIX).

   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 UNIX).
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`.

[1] cecil

```
DEFINE QLOCAL(QIN)
```

5. Nastavení 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
```

8. V produktu WebSphere Message Broker vytvořte tok zpráv pro směrování zpráv, které přicházejí do fronty alias 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 DEF a přiřaďte aliasu fronty 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 zprostředkovatele zpráv WebSphere Message Broker.
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 podobě produktem WebSphere Message Broker z alias fronty AIN . WebSphere Message Broker rozhoduje o tom, kam směrovat zprávu při čtení vlastnosti routeTo , která je stejně jako všechny vlastnosti nešifrovaná.

WebSphere Message Broker umístí zprávu na odpovídající 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-Zprostředkovatel zpráv může zobrazit obsah zprávy

Informace o této úloze

V tomto scénáři je skupině jednotlivců povoleno odesílat zprávy do zprostředkovatele zpráv WebSphere Message Broker. Jiná skupina je oprávněna přijímat zprávy, které jsou vytvořeny produktem WebSphere Message Broker. Přenos mezi stranami a produktem WebSphere Message Broker nemůže být odposlouchn.

Pamatujte si, že produkt WebSphere Message Broker přečte zásady a certifikáty ochrany pouze tehdy, když je fronta otevřena, takže musíte znovu načíst skupinu provádění po provedení jakýchkoli aktualizací zásad ochrany, aby změny nabyly platnosti.

```
mqsireload execution-group-name
```

Je-li produkt WebSphere Message Broker považován za oprávněnou osobu, která může číst nebo podepsat informační obsah zprávy, musíte nakonfigurovat produkt Advanced Message Security pro uživatele spouštějícího službu WebSphere Message Broker. Mějte na paměti, že se nejedná nutně o stejného uživatele, který vkládá/získává zprávy do front, ani na uživatele, který vytváří a implementuje aplikace WebSphere Message Broker.

Postup

1. Nakonfigurujte uživatele služby *alice*, *bob*, *cecil* a *dave* a uživatele služby WebSphere Message Broker tak, aby používal produkt Advanced Message Security , jak je popsáno v příručce **Quick Start Guide** (Windows nebo UNIX).

   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* do uživatele služby zprostředkovatele zpráv WebSphere Message Broker.

   To provedete extrakcí do externích souborů, každý z certifikátů, které identifikují *alice*, *bob*, *cecil* a *dave*, a pak přidá extrahované certifikáty do úložiště klíčů WebSphere Message Broker. Je důležité, abyste použili metodu popsanou v **Úloha 5. Sdílení certifikátů** v příručce **Quick Start Guide** (Windows nebo UNIX).
3. Zadejte certifikát uživatele služby zprostředkovatele zpráv WebSphere Message Broker do *alice*, *bob*, *cecil* a *dave*.

   Postupujte takto s použitím metody uvedené v předchozím kroku.

   Poznámka: *Alice* a *bob* potřebují uživatelský certifikát služby WebSphere Message Broker pro správné šifrování zpráv. Uživatel služby zprostředkovatele zpráv WebSphere Message Broker potřebuje certifikáty *alice's* a *bob* k ověření autorů zpráv. Uživatel služby zprostředkovatele zpráv WebSphere Message Broker potřebuje certifikáty *cecil's* a *dave* , aby pro ně šifroval zprávy. *cecil* a *dave* potřebují certifikát uživatele služby WebSphere Message Broker a ověřit, zda zpráva pochází z produktu WebSphere Message Broker.
4. Definujte lokální frontu s názvem `IN` a definujte zásadu zabezpečení s hodnotami *alice* a *bob* určenými jako autoři a uživatel služby WebSphere Message Broker určený 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 s uživatelem služby produktu WebSphere Message Broker určeným 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 WebSphere Message Broker 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 zprostředkovatele zpráv WebSphere Message Broker.
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 prostřednictvím produktu WebSphere Message Broker. WebSphere Message Broker bude přijímat zprávy pouze od *alice* a *bob* a odmítne všechny ostatní. Přijímané zprávy budou odpovídajícím způsobem zpracovány a poté podepsány a šifrovány pomocí klíčů *cecil* a *dave* před tím, než budou vloženy do výstupní fronty `OUT`. Pouze produkty *cecil* a *dave* jsou schopny jej číst, zprávy, které nejsou podepsány produktem WebSphere Message Broker, jsou odmítnuty.

Použití IBM WebSphere MQ Advanced Message Security s IBM WebSphere MQ Managed File Transfer

Tento scénář vysvětluje, jak nakonfigurovat produkt Advanced Message Security , aby poskytl utajení zpráv pro data odesílaná prostřednictvím produktu IBM WebSphere MQ Managed File Transfer.

Než začnete

Ujistěte se, že máte nainstalovanou komponentu Advanced Message Security na instalaci produktu WebSphere MQ hostící fronty používané produktem IBM WebSphere MQ Managed File Transfer , které chcete chránit.

Pokud se vaši agenti IBM WebSphere MQ Managed File Transfer připojují v režimu vazeb, ujistěte se, že máte nainstalovanou komponentu GSKit na lokální instalaci.

Informace o této úloze

Když dojde k přerušení přenosu dat mezi dvěma agenty IBM WebSphere MQ Managed File Transfer , potenciálně důvěrné data mohou zůstat nechráněná na základních frontách WebSphere MQ použitých ke správě přenosu. Tento scénář vysvětluje, jak nakonfigurovat a používat produkt Advanced Message Security k ochraně těchto dat ve frontách produktu IBM WebSphere MQ Managed File Transfer .

V tomto scénáři uvažujeme jednoduchou topologii zahrnující jeden počítač se dvěma frontami IBM WebSphere MQ Managed File Transfer a dvěma agenty, `AGENT1` a `AGENT2`, sdílením jednoho správce front, `hubQM`, jak je popsáno ve scénáři Základní přenos souboru pomocí skriptů. Oba agenti se připojují stejným způsobem, buď v režimu vazeb, nebo v režimu klienta.

1. Vytvoření certifikátů

Než začnete

Tento scénář používá jednoduchý model, ve kterém se uživatel `ftagent` ve skupině `FTAGENTS` používá ke spouštění procesů agenta IBM WebSphere MQ Managed File Transfer . 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 IBM WebSphere MQ Managed File Transfer spuštěni v režimu vazeb, jsou příkazy, které používáte k vytvoření úložiště klíčů CMS (Cryptographic Message Syntax), podrobně popsány v **Stručná úvodní příručka** (Windows nebo UNIX) pro vaši platformu.
- Pokud jsou agenti IBM WebSphere MQ Managed File Transfer spuštění v režimu klienta, příkazy, které budete potřebovat pro vytvoření JKS (Java Keystore), jsou podrobně popsány v "Stručná úvodní příručka pro klienty Java" na stránce 278.

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=IBM, L=Hursley, ST=Hampshire, C=GB
   ```

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 IBM WebSphere MQ 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=IBM,
   L=Hursley, ST=Hampshire, C=GB"
   -e AES128 -r "CN=ftagent, OU=MFT, O=IBM, L=Hursley, ST=Hampshire, C=GB"
   ```

3. Ujistěte se, že uživatel, který má spuštěný proces agenta IBM WebSphere MQ Managed File Transfer , má přístup k procházení fronty zásad systému 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 IBM WebSphere MQ 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.

instalaceIBM WebSphere MQ Advanced Message Security

Nainstalujte komponentu IBM WebSphere MQ Advanced Message Security na různých platformách.

Informace o této úloze

Kompletní instalační procedury naleznete v tématu Instalace produktu IBM WebSphere MQ Advanced Message Security.

Související úlohy

OdinstalaceIBM WebSphere MQ Advanced Message Security

Používání úložišť klíčů a certifikátů

Chcete-li zajistit transparentní ochranu šifrování pro aplikace WebSphere MQ , produkt Advanced Message Security použije soubor úložiště klíčů, kde jsou uloženy certifikáty veřejných klíčů a soukromý klíč.

V produktu Advanced Message Securityjsou uživatelé a aplikace představovány identitami infrastruktury veřejných klíčů (PKI). Tento typ identity se používá k podepisování a šifrování zpráv. Identita PKI je reprezentována polem **distinguished name (DN)** subjektu v certifikátu, který je přidružen k podepsaným a šifrovaným zprávám. Aby mohl uživatel nebo aplikace zašifrovat své zprávy, vyžadují přístup k souboru úložiště klíčů, kde jsou uloženy certifikáty a přidružené soukromé a veřejné klíče.

Umístění úložiště klíčů je poskytnuto v konfiguračním souboru úložiště klíčů, který je ve výchozím nastavení `keystore.conf` . Každý uživatel produktu Advanced Message Security musí mít konfigurační soubor úložiště klíčů, který ukazuje na soubor úložiště klíčů. Advanced Message Security přijímá následující formát souborů úložiště klíčů: `.kdb`, `.jceks`, `.jks`.

Standardní umístění souboru `keystore.conf` je:

- Na platformách UNIX : `$HOME/.mqs/keystore.conf`
- Na platformách Windows : *%HOMEDRIVE%%HOMEPATH%*`\.mqs\keystore.conf`

Používáte-li určený název souboru a umístění úložiště klíčů, měli byste použít následující příkazy:

- Pro Java: `java -D` *`MQS_KEYSTORE_CONF=path/filename app_name`*
- Pro klienta a server jazyka C:
  - V systému UNIX and Linux: `export MQS_KEYSTORE_CONF=`*`path/filename`*
  - V systému Windows: `set MQS_KEYSTORE_CONF=`*`path\filename`*

    Poznámka: Je-li k dispozici více než jedno písmeno jednotky, může cesta v systému Windows obsahovat písmeno jednotky.

Související pojmy

“Rozlišující názvy odesilatelů” na stránce 301
Rozlišující názvy (DN) odesilatelů identifikují uživatele, kteří mají oprávnění k umisťovat zprávy do fronty.

“Rozlišující názvy příjemců” na stránce 302
Rozlišovací jména (DN) příjemců identifikují uživatele, kteří mají oprávnění k načítání zpráv z fronty.

Struktura konfiguračního souboru úložiště klíčů (keystore.conf)

Konfigurační soubor úložiště klíčů (`keystore.conf`) ukazuje umístění produktu Advanced Message Security na umístění příslušného úložiště klíčů.

Existují dva typy konfigurace CMS a Java (JKS a JCEKS). Konfigurační záznamy CMS mají předponu `cms.` a Java mají předponu `jks.` nebo `jceks.` v závislosti na typu úložiště klíčů.

Konfigurační soubor, v závislosti na typu konfiguračního souboru, může mít jednu z následujících struktur:

```
cms.keystore = /<dir>/<keystore_file>
cms.certificate = certificate_label

jceks.keystore = <dir>/Keystore
jceks.certificate = <certificate_label>
jceks.encrypted = no
jceks.keystore_pass = <password>
jceks.key_pass = <password>
jceks.provider = IBMJCE

jks.keystore = <dir>/Keystore
jks.certificate = <certificate_label>
jks.encrypted = no
jks.keystore_pass = <password>
jks.key_pass = <password>
jks.provider = IBMJCE
```

Parametry konfiguračního souboru jsou definovány následujícím způsobem:

keystore
Cesta k souboru úložiště klíčů.

Důležité:

- Cesta k souboru úložiště klíčů nesmí obsahovat příponu souboru.
- V případě souborů úložiště klíčů Java produkt IBM WebSphere MQ AMS podporuje následující formáty souborů: `.jks`, `.jceks`, `.jck`.

certificate
Popisek certifikátu

encrypted
Stav hesla.

keystore_pass
Heslo pro soubor úložiště klíčů.

Poznámka:

- Pro úložiště klíčů CMS se produkt IBM WebSphere MQ AMS spoléhá na soubory pro dočasné ukládání (`.sth`), zatímco JKS a JCEKS mohou vyžadovat heslo jak pro certifikát, tak pro soukromý klíč uživatele.
- Ukládání hesel v prostém textu představuje bezpečnostní riziko.

key_pass
Heslo pro soukromý klíč uživatele.

Důležité: Ukládání hesel ve formě prostého textu může představovat bezpečnostní riziko.

provider
Poskytovatel zabezpečení Java, který implementuje kryptografické algoritmy vyžadované certifikátem úložiště klíčů.

Poznámka: Aktuálně je IBMJCE jediným poskytovatelem, který je podporován produktem Advanced Message Security.

Důležité: Informace uložené v úložišti klíčů jsou klíčové pro zabezpečený tok dat odeslaných pomocí produktu WebSphere MQ, což je důvod, proč administrátoři zabezpečení musí věnovat zvláštní pozornost při přiřazování oprávnění k souborům pro tyto soubory.

Zde je příklad souboru `keystore.conf` :

```
cms.keystore = c:\Documents and Settings\Alice\AliceKeystore
cms.certificate = AliceCert

jceks.keystore = c:/Documents and Settings/Alice/AliceKeystore
jceks.certificate = AliceCert
jceks.encrypted = no
jceks.keystore_pass = <password>
jceks.key_pass = <password>
jceks.provider = IBMJCE
```

Související úlohy

“Ochrana hesel v prostředí Java” na stránce 299
Uložení hesel úložiště klíčů a soukromých klíčů jako prostý text představuje bezpečnostní riziko, takže produkt Advanced Message Security poskytuje nástroj, který může tato hesla zakódovat pomocí klíče uživatele, který je k dispozici v souboru úložiště klíčů.

Promočování agenta MCA (Message Channel Agent)

Funkce MCA intercepce umožňuje správci front spuštěným pod produktem IBM WebSphere MQ selektivně povolit použití zásad pro kanály připojení serveru.

Funkce MCA intercepce umožňuje klientům, kteří zůstanou mimo produkt IBM WebSphere MQ AMS , stále být připojeni ke správci front a jejich zprávy, které mají být šifrovány a dešifrovány.

Funkce MCA interception je určena k poskytování funkcí produktu IBM WebSphere MQ AMS , když produkt IBM WebSphere MQ AMS nemůže být na straně klienta povolen. Všimněte si, že použití zachycení agenta MCA a klienta s povoleným produktem IBM WebSphere MQ AMSvede k dvojímu zabezpečení zpráv, které mohou být problematické pro příjem aplikací.

Je-li hlášena chyba 2085 (MQRC_UNKNOWN_OBJECT_NAME), používáte-li klienta produktu Version 7.5 nebo novější k připojení ke správci front z dřívější verze produktu, je třeba produkt IBM WebSphere MQ Advanced Message Security zakázat na straně klienta. Další informace viz "Zakázání produktu IBM WebSphere MQ Advanced Message Security na straně klienta" na stránce 292.

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 IBM WebSphere MQ AMS najdete v tématu "Používání úložišť klíčů a certifikátů" na stránce 288.

Chcete-li povolit zachycení agenta MCA, je třeba zadat název kanálu, který chcete použít v konfiguračním souboru úložiště klíčů. Pro zachycení agenta MCA lze použít pouze typ úložiště klíčů cms.

Příklad nastavení zachycování MCA naleznete v tématu "IBM WebSphere MQ AMS Příklad zachycení agenta MCA" na stránce 290.

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 WebSphere MQ AMS Příklad zachycení agenta MCA

Příklad úlohy, jak nastavit zachycení agenta MCA pro IBM WebSphere MQ 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.

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 Version 7.5byl produkt IBM WebSphere MQ AMS přídavným produktem, který měl být instalován odděleně a zachytávači byly nakonfigurovány pro ochranu aplikací. Od produktu Version 7.5 jsou 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 Version 7.5 nebo novější, způsobilo by to, že zpráva bude chráněna 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/mq75
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 UNIX).
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 Version 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 WebSphere MQ Version 7.5 :

```
/opt/mq75/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 WebSphere MQ Version 7.5 :

```
/opt/mqm/samp/bin/amqsgetc TESTQ TESTQMGR
```

Související úlohy

“Stručná úvodní příručka pro klienty Java” na stránce 278
Tato příručka slouží k rychlé konfiguraci produktu IBM Advanced Message Security k zajištění zabezpečení zpráv pro aplikace v jazyce Java, které se připojují s použitím vazeb klienta. Po dokončení této operace jste vytvořili úložiště klíčů k ověření identit uživatelů a definované zásady podepisování a šifrování pro správce front.

Související odkazy

“Známá omezení.” na stránce 266
Informace o omezeních produktu IBM WebSphere MQ Advanced Message Security.

Zakázání produktu IBM WebSphere MQ Advanced Message Security na straně klienta

Pokud používáte klienta produktu Version 7.5 nebo novější pro připojení ke správci front z dřívější verze produktu a je-li hlášena chyba 2085 (MQRC_UNKNOWN_OBJECT_NAME), je třeba v klientu vypnout produkt IBM WebSphere MQ Advanced Message Security (AMS).

Informace o této úloze

V produktu Version 7.5je produkt IBM WebSphere MQ Advanced Message Security (AMS) automaticky aktivován v klientovi IBM WebSphere MQ , takže se klient při výchozím nastavení pokouší zkontrolovat zásady zabezpečení pro objekty ve správci front. Avšak servery ve starších verzích produktu, například Version 7.1, nemají zpřístupněné AMS , což způsobí, že se ohlásí chyba 2085 (MQRC_UNKNOWN_TOBJECT_NAME) .

Je-li tato chyba hlášena při pokusu o připojení ke správci front ze starší verze produktu, můžete produkt AMS zakázat na klientovi následujícím způsobem:

- Pro klienty produktu Java lze následujícími způsoby:
  - V7.5.0.4 Nastavením proměnné prostředí AMQ_DISABLE_CLIENT_AMS.
  - V7.5.0.4 Nastavením systémové vlastnosti Java na hodnotu com.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS.
  - V7.5.0.5 Použitím vlastnosti DisableClientAMS, pod stanzou **Security** v souboru mqclient.ini .
- Pro klienty typu C platí jedním z následujících způsobů:
  - V7.5.0.4 Nastavením proměnné prostředí AMQ_DISABLE_CLIENT_AMS.
  - V7.5.0.5 Použitím vlastnosti DisableClientAMS, pod stanzou **Security** v souboru mqclient.ini .

Procedura

- Chcete-li zakázat produkt AMS na straně klienta, použijte jednu z následujících možností:

  V7.5.0.4 **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 klienta Version 7.5nebo novější, IBM WebSphere MQ classes for Java nebo klienta IBM WebSphere MQ classes for JMS .

Funkci AMQ_DISABLE_CLIENT_AMS můžete také použít k zakázání funkcí produktu AMS pro klienty jazyka C.

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
```

V 7.5.0.4 Systémová vlastnost com.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS

V případě klientů IBM WebSphere MQ classes for JMS a IBM WebSphere MQ classes for Java nastavte 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.

V 7.5.0.5 Vlastnost `DisableClientAMS` v souboru `mqclient.ini`

Pro klienty IBM WebSphere MQ classes for JMS a IBM WebSphere MQ classes for Java a pro klienty C přidejte název vlastnosti `DisableClientAMS` pod stanzou **`Security`** soubor `mqclient.ini` , jak je zobrazeno v následujícím příkladu:

```
Security:
DisableClientAMS=Yes
```

Můžete také povolit produkt AMS , jak je zobrazeno v následujícím příkladu:

```
Security:
DisableClientAMS=No
```

Jak pokračovat dále

Další informace o problémech s otevíráním chráněných front operačního systému AMS najdete v tématu “Problémy při otevírání chráněných front při použití JMS” na stránce 316.

Související pojmy

“Promočování agenta MCA (Message Channel Agent)” na stránce 289
Funkce MCA intercepce umožňuje správci front spuštěným pod produktem IBM WebSphere MQ selektivně povolit použití zásad pro kanály připojení serveru.

Související úlohy

Konfigurace klienta pomocí konfiguračního souboru

Související odkazy

Konfigurační soubor IBM WebSphere MQ classes for JMS

Požadavky na osvědčení 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 WebSphere MQ” na stránce 34.

Rozšíření použití klíče

Rozšíření pro použití klíče umístí další omezení na způsob, jakým lze použít certifikát.

V produktu Advanced Message Securitymusí být použití klíče nastaveno následujícím způsobem: pro certifikáty v normě X.509 V3 nebo novější, které se používají pro kvalitu ochrany integrity, jsou-li nastavena rozšíření použití klíče, musí obsahovat alespoň jednu z těchto dvou hodnot:

- **nonRepudiation**
- **digitalSignature**

For the quality of protection privacy, if the key usage extensions are set, they must also include the **keyEncipherment** extension.

Související pojmy

“Kvalita ochrany” na stránce 304
Advanced Message Security zásady ochrany dat znamenají kvalitu ochrany (QOP).

Metody ověření platnosti certifikátů v produktu IBM WebSphere MQ Advanced Message Security

Pomocí produktu IBM WebSphere MQ Advanced Message Security můžete zjišťovat a odmítat odvolané certifikáty, takže zprávy ve vašich frontách nebudou chráněny pomocí certifikátů, které nesplňují standardy zabezpečení.

Produkt IBM WebSphere MQ AMS umožňuje ověřit platnost certifikátu pomocí protokolu OCSP (Online Certificate Status Protocol) nebo seznamu odvolaných certifikátů (CRL).

Produkt IBM WebSphere MQ AMS lze nakonfigurovat buď pro kontrolu OCSP, nebo pro kontrolu CRL, nebo obojí. Jsou-li povoleny obě metody, pak z důvodu výkonu produkt IBM WebSphere MQ AMS nejprve použije protokol OCSP pro stav odvolání. Je-li stav odvolání certifikátu po kontrole OCSP neplatný, produkt IBM WebSphere MQ AMS použije kontrolu CRL.

Související pojmy

“Protokol OCSP (Online Certificate Status Protocol)” na stránce 294
Protokol OCSP (Online Certificate Status Protocol) určuje, zda byl certifikát odvolán, a proto pomáhá určit, zda je možné certifikát považovat za důvěryhodný.

“Seznamy odvolaných certifikátů (CRL)” na stránce 296
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)

Protokol OCSP (Online Certificate Status Protocol) určuje, zda byl certifikát odvolán, a proto pomáhá určit, zda je možné certifikát považovat za důvěryhodný.

Povolení kontroly OCSP v nativních zachytávačích

Chcete-li povolit kontrolu protokolu OCSP (Online Certificate Status Protocol) v produktu Advanced Message Security, musíte upravit konfigurační soubor úložiště klíčů.

Postup

Přidejte do konfiguračního souboru úložiště klíčů tyto volby:

Poznámka: Hodnoty uvedené v tabulce pro jednotlivé volby jsou výchozí.

Musíte zadat jednu z následujících hodnot:

- `ocsp.enable=on`
- `ocsp.url=<`*`reposnder_URL`*`>`
- `ocsp.http.proxy.host=<`*`OCSP_proxy`*`>`

Volba	Popis
`ocsp.enable=off`	Kontrolu OCSP povolte, má-li kontrolovaný certifikát rozšíření přístupu s informací o autoritě s přístupovou metodou, jež obsahuje identifikátor URI označující umístění odpovídacího modulu OCSP. Možné hodnoty: `on`/`off`.
`ocsp.url=<`*reposnder_URL*`>`	Adresa URL odpovídacího modulu OCSP.
`ocsp.http.proxy.host=<`*OCSP_proxy*`>`	Adresa URL serveru proxy OCSP.
`ocsp.http.proxy.port=<`*port_number*`>`	Číslo portu serveru proxy OCSP.
`ocsp.nonce.generation=on/off`	Generovat nonce (náhodně generované číslo) při dotazování OCSP. Výchozí hodnota: `off`.
`ocsp.nonce.check=on/off`	Kontrolovat nonce (náhodně generované číslo) po přijetí odezvy z OCSP. Výchozí hodnota: `off`.
`ocsp.nonce.size=8`	Velikost nonce (náhodně generovaného čísla) v bajtech.
`ocsp.http.get=on/off`	Určete operaci HTTP GET jako metodu svého požadavku. Je-li pro tuto volbu nastavena hodnota `off`, použije se metoda HTTP POST.
`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.

Povolení kontroly protokolu OCSP v jazyce Java
Chcete-li povolit vrácení protokolu OCSP pro jazyk 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 má nastaven AIA (Authority Information Access) (AIA).

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 Java, příliš dokončete konfiguraci, přidejte následující oprávnění jazyka 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 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)

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 certifikáty ověřit, 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.IBM WebSphere MQ AMS ověřuje cestu certifikátu pomocí algoritmu ověření PKIX. Když je řetěz vytvořen a ověřen, IBM WebSphere MQ 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 IBM WebSphere MQ AMS ověří, zda jsou nastaveny také **digitalSignature** nebo **nonRepudiation** . Pokud nejsou, je MQRC_SECURITY_ERROR ohlášen a zaprotokolován. Produkt IBM WebSphere MQ AMS dále stáhne seznamy CRL ze souborů nebo z LDAP v závislosti na tom, jaké hodnoty byly uvedeny v konfiguračním souboru. IBM WebSphere MQ AMSpodporuje pouze seznamy CRL, které jsou kódovány ve formátu DER. Není-li v konfiguračním souboru úložiště klíčů nalezena žádná konfigurace CRL, IBM WebSphere MQ AMS neprovede žádnou kontrolu platnosti CRL. U každého certifikátu CA se produkt IBM WebSphere MQ AMS dotazuje LDAP pro 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).

Postup

Přidejte do konfiguračního souboru následující volby:

Poznámka: Hodnoty uvedené v tabulce pro jednotlivé volby jsou výchozí.

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 jazyka Java produktu IBM WebSphere MQ AMS 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.
`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 IBM WebSphere MQ AMS vyprší časový limit.
`crl.http.cache_size=0`	Velikost mezipaměti HTTP, v bajtech.

Povolení podpory seznamu odvolaných certifikátů v jazyce Java
Chcete-li povolit podporu CRL v produktu Advanced Message Security, musíte upravit konfigurační soubor úložiště klíčů tak, aby produkt IBM WebSphere MQ 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 jazyka Java produktu IBM WebSphere MQ AMS úspěšně připojí k serveru LDAP, nedojde k pokusu o stažení seznamů CRL ze zbývajících serverů. 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.
`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.

Název vlastnosti	Popis
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 .

Ochrana hesel v prostředí Java

Uložení hesel úložiště klíčů a soukromých klíčů jako prostý text představuje bezpečnostní riziko, takže produkt Advanced Message Security poskytuje nástroj, který může tato hesla zakódovat pomocí klíče uživatele, který je k dispozici v souboru úložiště klíčů.

Než začnete

Vlastník souboru keystore.conf musí zajistit, aby oprávnění ke čtení souboru měl pouze vlastník souboru. Ochrana hesel popsaná v této kapitole je pouze dalším měřítkem ochrany.

Postup

1. Upravte soubory produktu keystore.conf tak, aby obsahovaly cestu k úložišti klíčů a uživatelům.

```
jceks.keystore = c:/Documents and Setting/Alice/AliceKeystore
jceks.certificate = AliceCert
jceks.provider = IBMJCE
```

2. Chcete-li spustit nástroj, zadejte:

```
java -cp com.ibm.mq.jmqi.jar com.ibm.mq.ese.config.KeyStoreConfigProtector keystore_password
private_key_password
```

Vygeneruje se výstup se zašifrovanými hesly a lze jej zkopírovat do souboru keystore.conf .

Chcete-li kopírovat výstup do souboru keystore.conf automaticky, spusťte:

```
java -cp com.ibm.mq.jmqi.jar com.ibm.mq.ese.config.KeyStoreConfigProtector keystore_password
private_key_password >> ~/<path_to_keystore>/keystore.conf
```

Poznámka:

Seznam výchozích umístění produktu keystore.conf na různých platformách naleznete v tématu “Používání úložišť klíčů a certifikátů” na stránce 288.

Příklad

Zde je příklad takového výstupu:

```
#Fri Jul 30 15:20:29 CEST 2010
jceks.key_pass=MMXh997n5ZOr8uRlJmc5qity9MN2CggGBMKCDxdbn1AyPklvdgTsOLG6X3C1YT7oDzwaqZFlOR4t\r\nm
Zsc7JGAx8nqqxLnAucdGn0NWo6xnjZB1n501YGol2k/
PhaQHhFXKMAU9dKg0f8djOtCAOlX4ETe\r\nfYl9LBUt2wk87uM7dSs\=
jceks.keystore_pass=OIdeayBnSCfLG4cFuxEVrk6SYyAsdSPpDqgPf16s9s1M04cqZjNbhgjoA2EXonudHZHH+4s2drvQ
```

```
\r\nCUvQgu9GuaBMJK2F2OjtHJJ1Y4BVeLW2c2okgawo/
W2J1AdUYKkJ0raYTkDouLaTYTQeulyG0xIl\r\niD2si1xUCxhYvvyhbbY\=
jceks.encrypted=yes
```

Správa zásad zabezpečení produktu IBM WebSphere MQ Advanced Message Security

Produkt IBM WebSphere MQ 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

Zásady zabezpečení produktu IBM 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” na stránce 304
Advanced Message Security zásady ochrany dat znamenají kvalitu ochrany (QOP).

“Atributy zásady zabezpečení” na stránce 303
Produkt Advanced Message Security můžete použít k výběru určitého algoritmu nebo metody k ochraně dat.

Název zásady

Název zásady je jedinečný název, který identifikuje určitou zásadu Advanced Message Security a frontu, na kterou se vztahuje.

Název zásady musí být stejný jako název fronty, na který se vztahuje. Mezi zásadou Advanced Message Security (IBM WebSphere MQ AMS) a frontou existuje mapování jedna ku jedné.

Když vytvoříte zásadu se stejným názvem jako fronta, aktivujete zásadu pro tuto frontu. Fronty bez odpovídajících názvů zásad nejsou chráněny produktem IBM WebSphere MQ 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

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.

Šifrovací algoritmus

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 zašifrované zprávy produktu Advanced Message Security 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

Atribut tolerování označuje, zda produkt IBM Advanced Message Security může 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

Rozlišující názvy (DN) odesilatelů identifikují uživatele, kteří mají oprávnění k umisťovat zprávy do fronty.

Produkt IBM Advanced Message Security (IBM WebSphere MQ AMS) nekontroluje, zda byla zpráva umístěna do fronty chráněné dat platným uživatelem, dokud se zpráva nenačte. Pokud zásada určuje jednoho či několik platných odesilatelů a uživatel, která zprávu zařadil do fronty, v seznamu platných odesilatelů uveden není, produkt IBM WebSphere MQ AMS v této fázi vrátí chybu pro aplikaci provádějící převzetí a zařadí zprávu do příslušné fronty chyb.

Pro zásadu může být určeno 0 či více rozlišujících názvů (DN) odesilatelů. Pokud pro zásadu nejsou určeny žádné rozlišující názvy odesilatelů, může do fronty zařazovat zprávy s ochranou dat kterýkoli uživatel s důvěryhodným certifikátem.

Tvar rozlišujících názvů odesilatelů je následující:

```
CN=Common Name,O=Organization,C=Country
```

Důležité:

- Všechny DN musí být velkými písmeny. Všechny identifikátory názvu komponenty v DN musí být uvedeny v pořadí uvedeném v následující tabulce:

Název komponenty	Hodnota
CN	Obecný název pro objekt tohoto DN, jako je úplný název nebo účel zařízení.

Název komponenty	Hodnota
OU	Jednotka v rámci organizace, se kterou je objekt DN přidružen, jako např. obchodní divize nebo název produktu.
O	Organizace, s níž je objekt DN přidružen, jako například korporace.
L	Lokalita (město nebo obec), kde je umístěn objekt DN.
ST	Název státu nebo provincie, kde je umístěn objekt DN.
C	Země, ve které je umístěn objekt rozlišovacího jména (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.
- IBM WebSphere MQ AMS podporuje DN s hodnotami pouze ze znakové sady Latin-1 . Chcete-li vytvořit DN se znaky sady, musíte nejprve vytvořit certifikát s DN, které je vytvořeno v kódování UTF-8 pomocí platformy UNIX s kódováním UTF-8 , nebo s obslužným programem iKeyman . Pak musíte vytvořit zásadu z platformy UNIX s kódováním UTF-8 zapnutým nebo pomocí modulu plug-in IBM WebSphere MQ AMS v produktu WebSphere MQ.

Související pojmy

“Rozlišující názvy příjemců” na stránce 302
Rozlišovací jména (DN) příjemců identifikují uživatele, kteří mají oprávnění k načítání zpráv z fronty.

Rozlišující názvy příjemců

Rozlišovací jména (DN) příjemců identifikují uživatele, kteří mají oprávnění k načítání zpráv z fronty.

Pro zásadu může být určeno nula či více rozlišujících názvů (DN) příjemců. Rozlišovací jména příjemců mají následující tvar:

```
CN=Common Name,O=Organization,C=Country
```

Důležité:

- Všechny DN musí být velkými písmeny. Všechny identifikátory názvu komponenty v DN musí být uvedeny v pořadí uvedeném v následující tabulce:

Název komponenty	Hodnota
CN	Obecný název pro objekt tohoto DN, jako je úplný název nebo účel zařízení.
OU	Jednotka v rámci organizace, se kterou je objekt DN přidružen, jako např. obchodní divize nebo název produktu.
O	Organizace, s níž je objekt DN přidružen, jako například korporace.
L	Lokalita (město nebo obec), kde je umístěn objekt DN.
ST	Název státu nebo provincie, kde je umístěn objekt DN.

Název komponenty	Hodnota
C	Země, ve které je umístěn objekt rozlišovacího jména (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.
- 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, které je vytvořeno v kódování UTF-8 pomocí platformy UNIX s kódováním UTF-8 , nebo s obslužným programem iKeyman . Pak musíte vytvořit zásadu z platformy UNIX s kódováním UTF-8 zapnutým nebo pomocí modulu plug-in Advanced Message Security v produktu WebSphere MQ.

Související pojmy

“Rozlišující názvy odesilatelů” na stránce 301
Rozlišující názvy (DN) odesilatelů identifikují uživatele, kteří mají oprávnění k umisťovat zprávy do fronty.

Atributy zásady zabezpečení

Produkt Advanced Message Security můžete použít k výběru určitého algoritmu nebo metody k ochraně dat.

Zásada zabezpečení je konceptuálním objektem, který popisuje způsob, jakým je zpráva šifrovaně šifrována a podepsána. Následující tabulka uvádí atributy zásady zabezpečení v produktu Advanced Message Security:

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

Advanced Message Security zásady ochrany dat znamenají kvalitu ochrany (QOP).

Tři úrovně ochrany v produktu Advanced Message Security závisí na kryptografických 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.
- 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 nestanovuje podpisový algoritmus nebo šifrovací algoritmus, má QOP typu NONE. Advanced Message Security neposkytuje žádnou ochranu dat pro fronty, které mají zásadu s QOP typu NONE.

Správa zásad zabezpečení

Zásada zabezpečení je konceptuálním objektem, který popisuje způsob, jakým je zpráva šifrovaně šifrována a podepsána.

Všechny administrativní úlohy související se zásadami zabezpečení se spouštějí z následujícího umístění:

- Na platformách UNIX : `<MQInstallRoot>/bin`
- Na platformách Windows lze administrativní úlohy spouštět z libovolného umístění, protože proměnná prostředí PATH se aktualizuje při instalaci.

Související úlohy

“Vytvoření zásad zabezpečení” na stránce 305
Zásady zabezpečení definují způsob, jakým je zpráva chráněna při vložení zprávy, nebo způsob, jakým musí být zpráva chráněna při přijetí zprávy.

“Změna zásad zabezpečení” na stránce 305
Pomocí produktu Advanced Message Security můžete změnit podrobnosti o zásadách zabezpečení, které jste již definovali.

“Zobrazení a výpis zásad zabezpečení” na stránce 306
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” na stránce 307
Chcete-li odebrat zásady zabezpečení v produktu Advanced Message Security, musíte použít příkaz `setmqspl` .

Vytvoření zásad zabezpečení

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 Pravidla pro pojmenování objektů WebSphere MQ.
- Chcete-li vytvořit zásadu zabezpečení, musíte mít potřebná oprávnění `+connect +inq +chg` . Úplnou syntaxi příkazu pro změnu oprávnění naleznete v tématu **`setmqaut`** .
- Ujistěte se, že máte nezbytná oprávnění k provozu ve frontách WebSphere MQ a ve správcích front. Další informace viz “Udělení oprávnění OAM” na stránce 309

Příklad

Zde je uveden příklad vytvoření zásady pro správce front `QMGR`. Zásada určuje, že zprávy mají být podepsány pomocí algoritmu `SHA1` 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 SHA1 -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 `DES` pro certifikáty s DN: `CN=jan, O=IBM, C=US` a `CN=jeff, O=IBM, C=US` a podepsána s algoritmem `MD5` pro certifikát s DN: `CN=phil, O=IBM, C=US`

```
$ setmqspl -m QMGR -p MY.OTHER.QUEUE -s MD5 -e DES -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

Změna zásad zabezpečení

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.
- Chcete-li vytvořit zásady zabezpečení, musíte mít nezbytná oprávnění produktu `+connect +inq +chg` . Úplnou syntaxi příkazu pro změnu oprávnění naleznete v tématu **`setmqaut`** .

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 budou šifrovány pomocí algoritmu RC2 pro certifikáty s DN:CN=bob, O=IBM, C=US a je podepsán algoritmem SHA1 pro certifikáty s DN:CN=C=jeff, O=IBM, C = US.

```
setmqspl -m QMGR -p MYQUEUE -e RC2 -s SHA1 -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 SHA1 -a CN=jeff,O=IBM,C=US -r CN=alice,O=IBM,C=US
```

Související odkazy

setmqspl

Zobrazení a výpis zásad zabezpečení

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 nezbytná oprávnění `+connect +inq +dsp` , která se použijí na správce front, aby bylo možné zobrazit a vypsat zásady zabezpečení. Úplnou syntaxi příkazu pro změnu oprávnění naleznete v tématu **`setmqaut`** .

Informace o této úloze

Následuje seznam příznaků příkazu `dspmqspl` :

Tabulka 27. Parametry příkazu `dspmqspl` .

Příznak příkazu	**Vysvětlení**
`-m`	Název správce front (**povinný**).
`-p`	Název zásady.
`-export`	Přidání tohoto parametru generuje výstup, který lze snadno použít na jiného správce front.

Příklad

V tomto příkladě vytvoříme dvě zásady zabezpečení pro `venus.queue.manager`:

```
setmqspl -m venus.queue.manager -p AMS_POL_04_ONE -s MD5 -a "CN=signer1,O=IBM,C=US" -e NONE
setmqspl -m venus.queue.manager -p AMS_POL_06_THREE -s MD5 -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: MD5
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: MD5
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: MD5
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 MD5 -a "CN=signer1,O=IBM,C=US" -e NONE

dspmqspl -m venus.queue.manager -export > policies.[bat|sh]
```

Chcete-li importovat zásady zabezpečení:

- Na platformách Windows spusťte příkaz `policies.bat` .
- Na platformách UNIX :
  1. Přihlaste se jako uživatel, který patří do skupiny administrace `mqm` WebSphere MQ .
  2. Zadejte příkaz `. policies.sh`.

Související odkazy

Úplný seznam atributů příkazu dspmqspl

Odebrání zásad zabezpečení

Chcete-li odebrat zásady zabezpečení v produktu Advanced Message Security, musíte použít příkaz `setmqspl` .

Než začnete

Existují některé vstupní podmínky, které musí být splněny při správě zásad zabezpečení:

- Správce front musí být spuštěn.
- Chcete-li vytvořit zásady zabezpečení, musíte mít nezbytná oprávnění produktu `+connect +inq +chg` . Úplnou syntaxi příkazu pro změnu oprávnění naleznete v tématu **`setmqaut`** .

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

Systémové fronty umožňují komunikaci mezi produktem WebSphere MQ a jeho pomocnými aplikacemi. Kdykoli je vytvořen správce front, vytvoří se také systémová fronta pro ukládání interních zpráv a dat produktu WebSphere MQ . Systémové fronty můžete chránit pomocí produktu Advanced Message Security tak, aby k nim mohli přistupovat nebo dešifrovat pouze autorizovaní uživatelé.

Ochrana systémové fronty se řídí stejným vzorem jako ochrana běžných front. Viz “Vytvoření zásad zabezpečení” na stránce 305.

Chcete-li použít ochranu systémové fronty na platformách Windows , zkopírujte soubor `keystore.conf` do následujícího adresáře:

```
c:\Documents and Settings\Default User\.mqs\keystore.conf
```

K zajištění ochrany pro produkt `SYSTEM.ADMIN.COMMAND.QUEUE`musí mít příkazový server přístup k serveru `keystore` a `keystore.conf`, který obsahuje klíče a konfiguraci, aby mohl příkazový server získat přístup ke 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 povolené podepisující subjekty, zprávy příkazu, které neprojdou kontrolou rozlišujícího názvu (DN) podepsaného, 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 produktu WebSphere MQ Explorer, nejsou chráněny produktem WebSphere MQ AMS.

Změny zásad zabezpečení produktu Advanced Message Security vyžadují restartování příkazového serveru WebSphere MQ

Zásady zabezpečení nemají vliv na následující fronty SYSTEM:

- SYSTEM.ADMIN.ACCOUNTING.QUEUE
- SYSTEM.ADMIN.ACTIVITY.QUEUE
- SYSTEM.ADMIN.CHANNEL.EVENT
- SYSTEM.ADMIN.COMMAND.EVENT
- 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
- SYSTEM.BROKER.CONTROL.QUEUE
- SYSTEM.BROKER.DEFAULT.STREAM
- SYSTEM.BROKER.INTER.BROKER.COMMUNICATIONS
- SYSTEM.CHANNEL.INITQ
- SYSTEM.CHANNEL.SYNCQ
- SYSTEM.CICS.INITIATION.QUEUE
- SYSTEM.CLUSTER.COMMAND.QUEUE

- SYSTEM.CLUSTER.HISTORY.QUEUE
- SYSTEM.CLUSTER.REPOSITORY.QUEUE
- SYSTEM.CLUSTER.TRANSMIT.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
- SYSTEM.PENDING.DATA.QUEUE
- SYSTEM.PROTECTION.ERROR.QUEUE
- SYSTEM.PROTECTION.POLICY.QUEUE
- SYSTEM.RETAINED.PUB.QUEUE
- SYSTEM.SELECTION.EVALUATION.QUEUE
- SYSTEM.SELECTION.VALIDATION.QUEUE

Udělení oprávnění OAM

Oprávnění k souboru autorizují všechny uživatele k provedení příkazů `setmqspl` a `dspmqspl` . Produkt IBM 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 WebSphere 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
```

Události příkazů a konfigurace

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 WebSphere MQ jsou zprávami o formátu PCF odeslaným do vyhrazených front.

Zprávy událostí konfigurace jsou odeslány na SYSTEM.ADMIN.CONFIG.EVENT ve správci front, ve kterém došlo k události.

Zprávy událostí příkazu se odesílají do SYSTEM.ADMIN.COMMAND.EVENT ve správci front, ve kterém došlo k události.

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” na stránce 305, které generují dvě zprávy událostí produktu WebSphere MQ :

  - Událost konfigurace
  - Událost příkazu
- "Změna zásad zabezpečení" na stránce 305, který generuje tři zprávy událostí produktu WebSphere MQ :
  - Událost konfigurace, která obsahuje staré hodnoty zásad zabezpečení
  - Událost konfigurace, která obsahuje nové hodnoty zásad zabezpečení
  - Událost příkazu
- Produkt "Zobrazení a výpis zásad zabezpečení" na stránce 306, který generuje jednu zprávu události produktu WebSphere MQ :
  - Událost příkazu
- "Odebrání zásad zabezpečení" na stránce 307, který generuje dvě zprávy událostí produktu WebSphere MQ :
  - Událost konfigurace
  - Událost příkazu

Povolení a zakázání protokolování událostí

Pomocí atributů správce front CONFIGEV a CMDEV můžete řídit události příkazů a konfiguračních událostí. 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 parametr 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 příkazové události pro příkazy s výjimkou příkazů DISPLAY MQSC a Inquire PCF, nastavte parametr CMDEV na NODISPLAY. 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 Websphere MQ

Formát zprávy události příkazu

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 se vždy nacházejí dva parametry typu MQCFGR (skupiny). 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 průzkumníka produktu WebSphere 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: 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.

EventIdentityData

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.

Command

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 WebSphere MQ 7.5 `cmqcfc.h`

Vráceno: Jako vždycky.

Příkaz CommandData obsahuje prvky PCF, které obsahují příkaz PCF.

Formát zprávy události konfigurace

Události konfigurace jsou zprávy PCF standardního formátu produktu Advanced Message Security .

Možné hodnoty deskriptoru zpráv MQMD naleznete v tématu Zpráva události MQMD (deskriptor zprávy).

Zde jsou vybrané hodnoty MQMD:

```
Format = MQFMT_EVENT
Peristence = MQPER_PERSISTENCE_AS_Q_DEF
PutApplType = MQAT_QMGR                      //for both CLI and command server
```

Vyrovnávací paměť zpráv se skládá z struktury MQCFH a struktury parametrů, která za ní následuje. Možné hodnoty MQCFH naleznete v části Zpráva události MQCFH (záhlaví PCF).

Zde jsou vybrané hodnoty MQCFH:

```
Type = MQCFT_EVENT
Command = MQCMD_CONFIG_EVENT
MsgSeqNumber = 1 or 2          // 2 will be in case of Change Object event
Control = MQCFC_LAST or MQCFC_NOT_LAST     //MQCFC_NOT_LAST will be in case of 1 Change Object
event
ParameterCount = reflects number of PCF parameters following MQCFH
CompCode = MQCC_WARNING
Reason = one of {MQRC_CONFIG_CREATE_OBJECT, MQRC_CONFIG_CHANGE_OBJECT,
MQRC_CONFIG_DELETE_OBJECT}
```

Parametry následující MQCFH jsou:

EventUserID

Popis: ID uživatele, pod kterým byl spuštěn příkaz nebo volání, které událost vygenerovalo. (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 SID systému Windows 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
Zpráva příkazu z modulu plug-in průzkumníka WebSphere 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 produktu WebSphere MQ 7.5 nebo v souboru `cmqc.h` .

Vráceno: Jako vždycky.

PolicyName

Popis: Název zásady Advanced Message Security .

Identifikátor: **MQCA_POLICY_NAME**.

Datový typ: MQCFST.

Hodnota: **2112** -Číselná hodnota definovaná v produktu WebSphere MQ 7.5 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 produktu WebSphere MQ 7.5 nebo v souboru `cmqc.h` .

Vráceno: Vždy

TolerateFlag

Popis: Příznak tolerance zásad produktu Advanced Message Security .

Identifikátor: **Objekt MQIA_TOLEERATE_UNPROTECTED**

Datový typ: MQCFIN

Hodnota **235** -číselná hodnota definovaná v produktu WebSphere MQ 7.5 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 produktu WebSphere MQ 7.5 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 produktu WebSphere MQ 7.5 nebo v souboru `cmqc.h` .
Vráceno:	Kdykoli je definován šifrovací algoritmus v zásadě WebSphere MQ

SignerDNs

Popis:	Předmět DistinguishedName povolených podepisujících subjektů.
Identifikátor:	**ROZLIŠUJÍCÍ NÁZEV MQCA_SIGNERDN**
Datový typ:	MQCFSL
Hodnota:	**2113** -Číselná hodnota definovaná v produktu WebSphere MQ 7.5 nebo v souboru `cmqc.h` .
Maximální délka:	Nejdelší rozlišující název podepisujícího subjektu v zásadě, ale ne déle než MQ_DISTINGUISHED_NAME_LENGTH
Vráceno:	Kdykoli jsou definovány v zásadě WebSphere MQ .

RecipientDNs

Popis:	Předmět DistinguishedName povolených podepisujících subjektů.
Identifikátor:	**MQCA_RECIPIENT_DN**
Datový typ:	MQCFSL
Hodnota:	**2114** -Číselná hodnota definovaná v produktu WebSphere MQ 7.5 nebo v souboru `cmqc.h` .
Maximální délka:	Nejdelší rozlišující název příjemce v zásadě, ale již není MQ_DISTINGUISHED_NAME_LENGTH.
Vráceno:	Kdykoli jsou definovány v zásadě WebSphere MQ .

Problémy a řešení

Tento oddíl popisuje, jak vyřešit problémy, které mohou nastat při instalaci produktu IBM Tyto informace použijte k identifikaci a vyřešení problémů souvisejících s produktem Advanced Message Security.

com.ibm.security.pkcsutil.PKCSException: Chyba šifrování obsahu

Chyba `com.ibm.security.pkcsutil.PKCSException: Error encrypting contents` napovídá, že produkt IBM Advanced Message Security má problémy s přístupem k šifrovacím algoritmům.

Pokud Advanced Message Securityvrátí následující chybu:

```
DRQJP0103E   The IBM WebSphere MQ Advanced Message Security Java interceptor failed to protect
message.
  com.ibm.security.pkcsutil.PKCSException: Error encrypting contents
(java.security.InvalidKeyException: Illegal key size or default parameters)
```

ověřit, zda zásada zabezpečení JCE v produktu `JAVA_HOME/lib/security/local_policy.jar/*.policy` uděluje přístup k podpisovým algoritmům používaným v zásadě AMS produktu MQ .

Není-li algoritmus podpisu, který chcete použít, uveden v aktuální zásadě zabezpečení, stáhněte správný soubor zásad Java z následujících umístění:

- Soubory zásad sady SDK společnosti IBM pro jazyk Java 1.4.2.
- Soubory zásad sady SDK společnosti IBM pro jazyk Java 5.0.
- Soubory zásad sady SDK společnosti IBM pro prostředí Java 6.0.
- Soubory zásad sady SDK společnosti IBM pro prostředí Java 7.0.

Podpora OSGi

Chcete-li použít svazek balíků OSGi s dalšími parametry IBM Advanced Message Security , jsou vyžadovány další parametry.

Spusťte následující parametr během spuštění svazku balíků OSGi:

```
-Dorg.osgi.framework.system.packages.extra=com.ibm.security.pkcs7
```

Když používáte šifrované heslo ve vašem keystore.conf, musí být přidán následující příkaz, když je spuštěn balík OSGi:

```
-Dorg.osgi.framework.system.packages.extra=com.ibm.security.pkcs7,com.ibm.misc
```

Omezení: Produkt IBM WebSphere MQ AMS podporuje komunikaci pouze pomocí základních tříd Java produktu MQ pro fronty chráněné v rámci svazku balíků OSGi.

Problémy při otevírání chráněných front při použití JMS

Různé problémy se mohou vyskytnout při otevření chráněných front při použití produktu IBM WebSphere MQ Advanced Message Security.

Spouštím produkt JMS a obdržíte chybu 2085 (MQRC_UNKNOWN_OBJECT_NAME) spolu s chybou JMSMQ2008.

Ověřili jste, že jste nastavili IBM WebSphere MQ Advanced Message Security , jak je popsáno v “Stručná úvodní příručka pro klienty Java” na stránce 278.

Možnou příčinou je to, že používáte prostředí JRE (non-IBM Java Runtime Environment). Jedná se o známé omezení popsané v “Známá omezení.” na stránce 266.

Nenastavili jste proměnnou prostředí AMQ_DISABLE_CLIENT_AMS.

Řešení problému

Pro práci s tímto problémem jsou k dispozici čtyři možnosti:

1. Spusťte aplikaci produktu JMS v rámci podporovaného běhového prostředí produktu IBM Java (JRE).
2. Přesuňte aplikaci na stejný počítač, na kterém je spuštěn správce front, a připojte se k němu pomocí připojení v režimu vázání.

   Připojení v režimu vazeb používá nativní knihovny platformy k provádění volání rozhraní API produktu IBM WebSphere MQ . Proto se nativní zachytávač AMS používá k provádění operací AMS a neexistuje žádné spoléhání se na schopnosti prostředí JRE.

3. Použijte zachytávač MCA, protože umožňuje podepisování a šifrování zpráv ihned po jejich příchodu do správce front, aniž by bylo nutné, aby klient prováděl jakékoli zpracování AMS.

   Vzhledem k tomu, že je ochrana použita ve správci front, musí být použit alternativní mechanizmus k ochraně zpráv v režimu přenosu od klienta ke správci front. Nejčastěji je toto dosaženo konfigurací šifrování SSL/TLS na kanálu připojení serveru použitého aplikací.
4. Nastavte proměnnou prostředí AMQ_DISABLE_CLIENT_AMS, nechcete-li používat produkt IBM WebSphere MQ Advanced Message Security.

Další informace viz "Promočování agenta MCA (Message Channel Agent)" na stránce 289.

Poznámka: Musí existovat zásada zabezpečení pro každou frontu, do které bude program MCA Interceptor doručovat zprávy. Jinými slovy, cílová fronta musí mít zásadu zabezpečení AMS na místě s rozlišujícím názvem (DN) podepsaného a příjemcem shodujícím se s certifikátem přiřazeným k Interceptor MCA. To znamená, že DN certifikátu určeného vlastností `cms.certificate.channel.SYSTEM.DEF.SVRCONN` v rámci `keystore.conf` používaného správcem front.

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, je-li poskytnuta, vám pomohou 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 IBM 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 (http://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: