

8.0

*Zabezpečení produktu IBM MQ*

**IBM**

**Poznámka**

Než začnete používat tyto informace a produkt, který podporují, přečtěte si informace, které uvádí [“Poznámky” na stránce 521](#).

Toto vydání se vztahuje na verzi 8 vydání IBM® MQ a na všechna následná vydání a modifikace, 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.

© **Copyright International Business Machines Corporation 2007, 2023.**

---

# Obsah

<b>Zabezpečení.....</b>	<b>5</b>
přehled zabezpečení.....	5
Bezpečnostní koncepce a mechanismy.....	5
IBM MQ mechanismy zabezpečení.....	20
Plánování bezpečnostních požadavků.....	67
Plánování identifikace a ověření.....	68
Plánování autorizace.....	71
Plánování utajení.....	86
Plánování integrity dat.....	93
Plánování monitorování.....	94
Plánování zabezpečení podle topologie.....	95
Brány firewall a přímý průchod na Internet.....	109
Kontrolní seznam implementace zabezpečení produktu IBM MQ for z/OS.....	109
Nastavení zabezpečení.....	112
Nastavení zabezpečení v systémech Windows, SYSTÉM UNIX a Linux.....	112
Nastavení zabezpečení v systému HP Integrity NonStop Server.....	141
Nastavení zabezpečení v systému IBM i.....	142
Nastavení zabezpečení v systému z/OS.....	171
Nastavení zabezpečení produktu IBM MQ MQI client.....	254
Nastavení komunikace pro SSL nebo TLS v systému IBM i.....	257
Nastavení komunikace pro zabezpečení SSL nebo TLS v systémech UNIX, Linux nebo Windows.....	257
Nastavení komunikace pro SSL nebo TLS v systému z/OS.....	258
Práce s SSL nebo TLS.....	259
Identifikace a ověřování uživatelů.....	315
Oprávnění uživatelé.....	318
Identifikace a ověřování uživatelů pomocí struktury MQCSP.....	319
Implementace identifikace a ověření v uživatelských procedurách zabezpečení.....	319
Mapování identit ve výstupních procedurách zprávy.....	320
Mapování identity ve výstupu rozhraní API a ukončení přeletu rozhraní API.....	321
Práce se zrušenými certifikáty.....	322
Použití metody PAM (Pluggable Authentication Method).....	333
Autorizace přístupu k objektům.....	333
Řízení přístupu k objektům pomocí OAM v systémech UNIX, Linux a Windows.....	334
Udělení požadovaného přístupu k prostředkům.....	343
Oprávnění k administraci produktu IBM MQ v systémech SYSTÉM UNIX, Linux a Windows.....	377
Oprávnění pro práci s objekty IBM MQ v systémech UNIX, Linux a Windows.....	379
Implementace řízení přístupu v uživatelských procedurách zabezpečení.....	384
Implementace řízení přístupu ve výstupních procedurách zprávy.....	385
Implementace řízení přístupu ve výstupu rozhraní API a ukončení přeletu rozhraní API.....	386
Přehled autorizace LDAP.....	386
Nastavení oprávnění.....	388
Zobrazení autorizací.....	389
Další pokyny při použití autorizace LDAP.....	390
Přepínání mezi modely autorizace OS a LDAP.....	391
Administrace LDAP.....	392
Důvěrnost zpráv.....	392
Povolení specifikace CipherSpecs.....	393
Resetování tajných klíčů SSL a TLS.....	400
Implementace utajení v uživatelských ukončovacích programech.....	401
Integrita dat zpráv.....	403
Auditování.....	403
Uchování zabezpečených klastrů.....	404

Zastavení neautorizovaných správců front při odesílání zpráv.....	404
Zastavení neautorizovaných správců front při vkládání zpráv do front.....	404
Autorizace vkládání zpráv ve vzdálených frontách klastru.....	405
Zabránění připojování správců front ke klastru.....	406
Vynucení opuštění klastru nechtěným správcům front.....	407
Zabránění příjmu zpráv správcem front.....	408
SSL a klastry.....	408
Zabezpečení publikování/odběru.....	410
Příklad nastavení zabezpečení pro publikování/odběr.....	417
Zabezpečení odběru.....	430
Zabezpečení publikování/odběru mezi správci front.....	432
Ochrana podrobností ověření databáze.....	435
Zabezpečení klientů AMQP.....	436
Omezení převzetí klienta AMQP.....	438
IBM MQ Advanced Message Security.....	438
Přehled produktu IBM MQ AMS.....	439
instalace IBM MQ Advanced Message Security.....	463
Auditování na z/OS.....	464
Používání úložišť klíčů a certifikátů.....	465
Zásady zabezpečení.....	488
Problémy a řešení.....	508
Příklady konfigurací v systému z/OS.....	510
<b>Poznámky.....</b>	<b>521</b>
Informace o programovacím rozhraní.....	522
Ochranné známky.....	522

# Zabezpečení

---

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

## přehled zabezpečení

---

Tato kolekce témat představuje koncepte zabezpečení produktu IBM MQ .

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

## Bezpečnostní koncepte a mechanismy

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

Běžně přijímaná bezpečnostní opatření jsou následující:

- [“Identifikace a ověřování” na stránce 5](#)
- [“Autorizace” na stránce 6](#)
- [“Auditování” na stránce 6](#)
- [“Důvěrnost” na stránce 6](#)
- [“Integrita dat” na stránce 7](#)

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

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

Plánujete-li implementaci produktu IBM MQ , zvažte, které bezpečnostní mechanismy vyžadují, abyste implementovali ty aspekty zabezpečení, které jsou pro vás důležité. Další informace o tom, co byste měli zvážit po přečtení těchto témat, najdete v tématu [“Plánování bezpečnostních požadavků” na stránce 67](#).

### Související pojmy

[“Práce s SSL nebo TLS” na stránce 259](#)

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

### Související informace

[Připojení dvou správců front s použitím zabezpečení SSL nebo TLS](#)

## Identifikace a ověřování

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

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

## Neodmítání

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

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

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

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

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

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

### Související pojmy

[“Identifikace a ověření v produktu IBM MQ” na stránce 20](#)

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

## Autorizace

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

### Související pojmy

[“Autorizace v produktu IBM MQ” na stránce 21](#)

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

## Auditování

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

Další informace o tom, jak nastavit autorizaci, najdete v tématu [“Plánování autorizace” na stránce 71](#) a přidružených dílčích tématech.

### Související pojmy

[“Auditování v IBM MQ” na stránce 21](#)

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

## Důvěrnost

Služba *confidentiality* chrání citlivé informace před neoprávněným zveřejněním.

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

Šifrovat citlivá data při přenosu po komunikační síti, zejména v nezabezpečené síti, jako je například Internet. V síťovém prostředí nejsou mechanismy 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 mechanismy 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.

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

## Koncepce šifrování

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

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

### Související pojmy

“Šifrování v produktu IBM MQ” na stránce 22

IBM 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 následujícími způsoby:

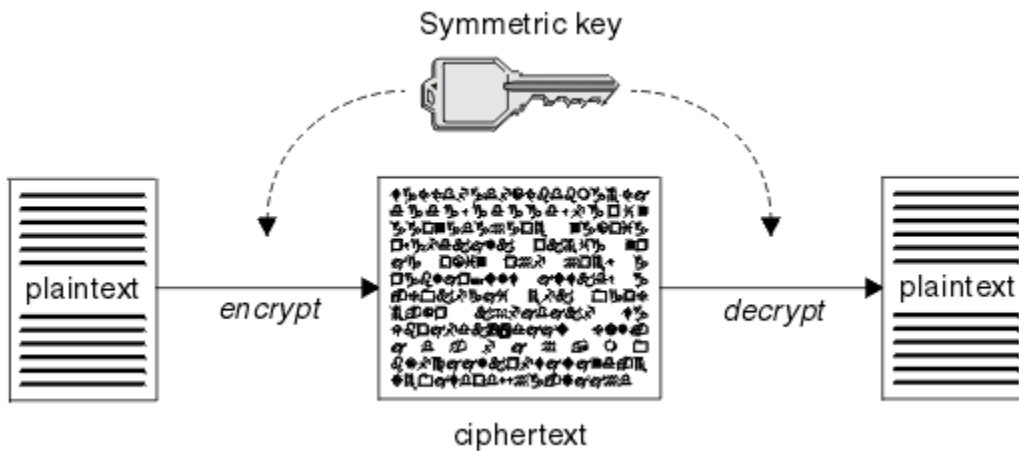
1. Odesílatel převádí zprávu prostého textu na šifrovaný text. Tato část procesu se nazývá *šifrování* (někdy *encipherment*).
2. Šifrovací text se přenáší do příjemce.
3. Příjemce převádí zprávu šifrovaného textu zpět na její prostý textový tvar. Tato část procesu se nazývá *dešifrování* (někdy *dešifrovací*).

Převod zahrnuje posloupnost matematických operací, které mění vzhled zprávy během přenosu, ale nemají vliv na obsah. Kryptografické techniky mohou zajistit důvěrnost a ochranu zpráv proti neoprávněnému prohlížení (odposlouchávání), protože šifrovaná zpráva není srozumitelná. Digitální podpisy, které poskytují záruku integrity zpráv, používají šifrovací techniky. Další informace viz [“Digitální podpisy v SSL a TLS”](#) na stránce 19.

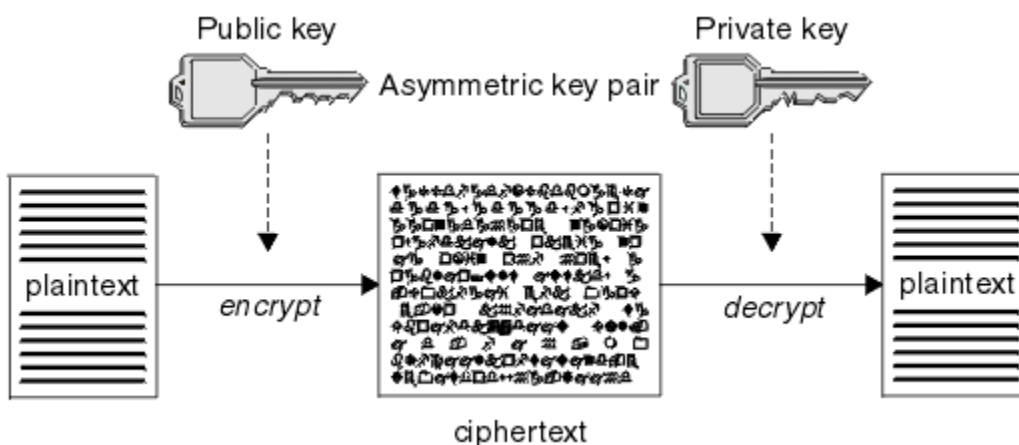
Kryptografické techniky zahrnují obecný algoritmus, který je specifický pro použití klíčů. Existují dvě třídy algoritmu:

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

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



Obrázek 1. šifrování pomocí symetrických klíčů



Obrázek 2. šifrování pomocí asymetrických klíčů

Obrázek 2 na stránce 8 uvádí prostý text zašifrovaný pomocí veřejného klíče příjemce a dešifrován pomocí soukromého klíče příjemce. Soukromý klíč pro dešifrování šifrovaného textu obsahuje pouze určený příjemce. Všimněte si, že odesílatel 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 dlouhé. Blokované algoritmy jsou obvykle pomalejší než proudové algoritmy.

### **Algoritmus šifry proudu**

Tyto algoritmy fungují na každém bajtu dat. Algoritmy proudů jsou obvykle rychlejší než blokované algoritmy.

### **Digesty zpráv a digitální podpisy**

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

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

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

Kód digest zprávy se odešle se zprávou samotnou. Příjemce může vygenerovat kód digest pro zprávu a porovnat jej s použitím kódu digest odesílatele. 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 19](#)

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

### **digitální certifikáty**

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

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

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

Pokud jsou veřejné klíče odeslány přímo jejich vlastníkem do jiné entity, je zde riziko, že zpráva bude zachycena a veřejný klíč nahradí jiným. Tento stav je znám jako *muž uprostřed útoku*. Řešením tohoto problému je výměna veřejných klíčů prostřednictvím důvěryhodné třetí strany, což vám dává silné ujištění, že veřejný klíč skutečně patří k subjektu, s nímž komunikujete. Místo přímého odeslání svého veřejného klíče se obraťte na důvěryhodnou třetí stranu, aby ji začlenila do digitálního certifikátu. Důvěryhodná třetí strana, která vydává digitální certifikáty, se nazývá certifikační autorita (CA), jak je popsáno v [“Vydavatelé certifikátů” na stránce 10](#).

*Co je v digitálním certifikátu*

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

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

Digitální certifikáty obsahují alespoň následující informace o certifikovaném subjektu:

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

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

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

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

#### *Požadavky na osobní certifikáty*

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

Protože IBM MQ je 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 MQ naleznete v tématu [“Zásady ověření platnosti certifikátu v produktu IBM MQ”](#) na stránce 43.

#### *Vydavatelé certifikátů*

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

Role CA jsou:

- Při přijetí požadavku na digitální certifikát ověřit identitu žadatele před sestavením, podepsáním a vrácením osobního certifikátu
- Zajištění vlastního veřejného klíče vydavatele certifikátů ve svém certifikátu CA
- Chcete-li publikovat seznamy certifikátů, které již nejsou důvěryhodné v seznamu odvolaných certifikátů (CRL). Další informace naleznete v tématu [“Práce se zrušenými certifikáty”](#) na stránce 322
- Zajištění přístupu k stavu odvolání certifikátu pomocí fungování serveru odpovídacího modulu OCSP

## Rozlišující názvy

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



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

Typ atributu	Popis
SERIALNUMBER	Sériové číslo certifikátu
MAIL	E-mailová adresa
E	E-mailová adresa (zamítnuto ve prospěch volby MAIL)
UID nebo USERID	Identifikátor uživatele
CN	Obecný název
T	Titulek
OU	Název organizační jednotky
DC	Komponenta domény
O	Název organizace
STREET	Ulice/první řádek adresy
L	Název umístění
ST (nebo SP či S)	Název státu nebo správního celku
PC	PSČ
C	Země
UNSTRUCTUREDNAME	Název hostitele
UNSTRUCTUREDADDRESS	Adresa IP
DNQ	Kvalifikátor rozlišujícího názvu

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

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

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

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

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

IBM MQ toleruje určité poškozené DN. Další informace viz [IBM MQ pravidla pro hodnoty SSLPEER](#).

### Související pojmy

“Co je v digitálním certifikátu” na stránce 9

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).

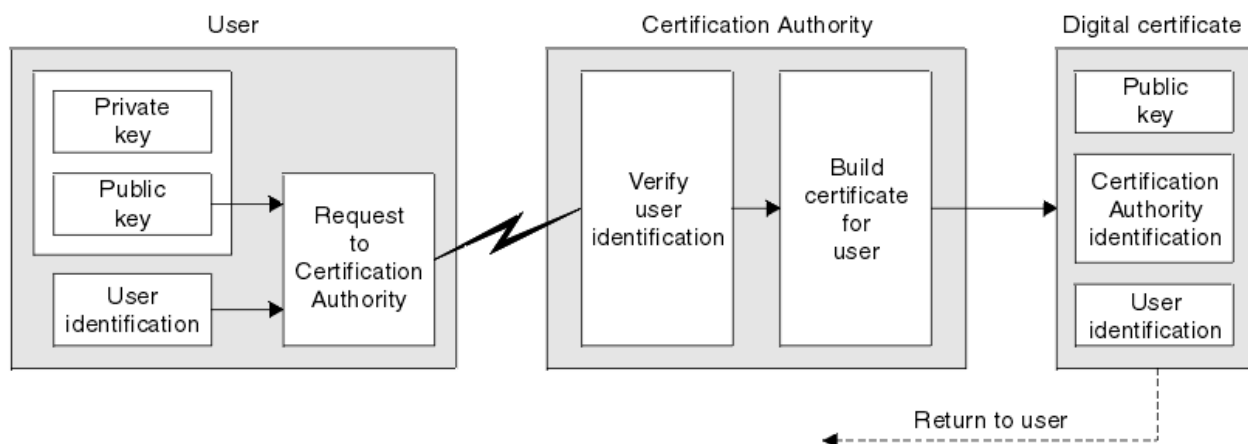
Digitální certifikát získáte odesláním informací do CA ve formě žádosti o certifikát. Standard X.509 definuje formát pro tyto informace, ale některé CA mají svůj vlastní formát. Požadavky na certifikáty jsou typicky generovány nástrojem pro správu certifikátů, který váš systém používá; například:

- **distributed** **IBM i** Nástroj Te iKeyman na systémech UNIX, Linux® a Windows
- **z/OS** RACF v systému z/OS.

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

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

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



Obrázek 3. Získání digitálního certifikátu

V diagramu:

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

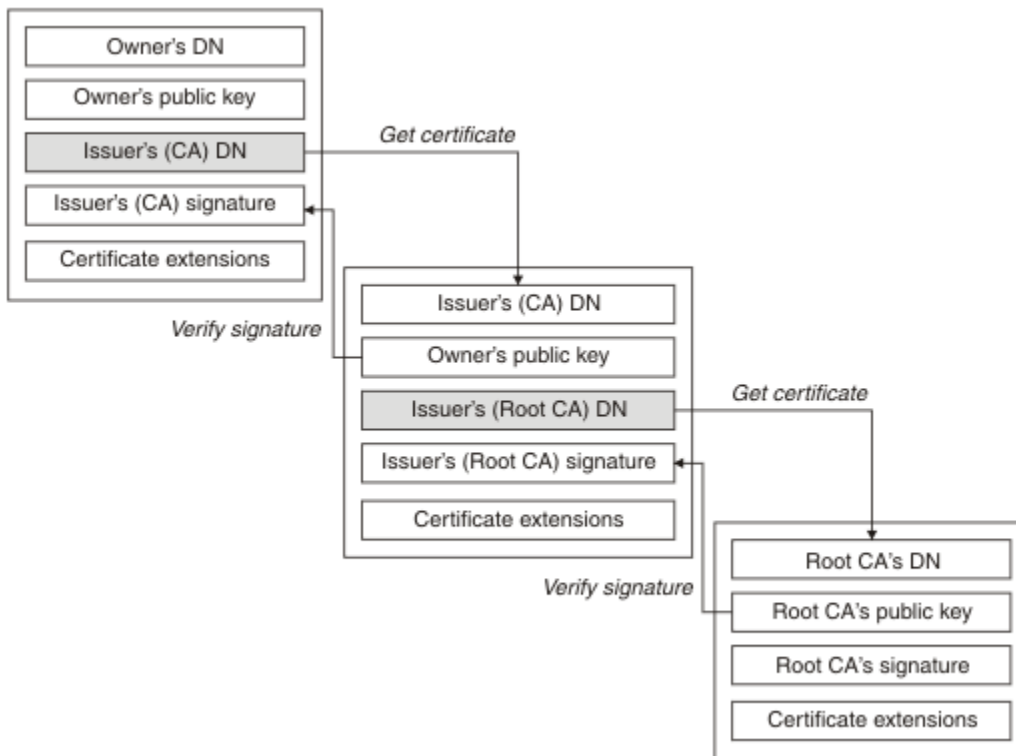
Digitální certifikáty obsahují jiná pole než ta, která jsou uvedena v diagramu. Další informace o ostatních polích v digitálním certifikátu viz ["Co je v digitálním certifikátu"](#) na stránce 9.

#### Způsob práce řetězců certifikátů

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

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

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



Obrázek 4. Linie důvěry

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

#### *Když certifikáty již nejsou platné*

Digitální certifikáty mohou vypršet nebo zrušit jejich platnost.

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

Certifikáty mohou být odvolány z různých důvodů včetně:

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

IBM 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 mít přístup k seznamu odvolaných certifikátů (CRL) na serveru LDAP. Informace o odvolání OCSP a CRL jsou publikovány vydavatelem certifikátů. Další informace viz [“Práce se zrušenými certifikáty”](#) na stránce 322.

### **infrastruktura veřejných klíčů (PKI)**

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

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

- Vydávání digitálních certifikátů
- Ověření digitálních certifikátů
- Zrušení platnosti digitálních certifikátů
- Distribuce veřejných klíčů

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

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

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

## Kryptografické 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 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 nespolečně spolupracují.

### Související pojmy

“Protokoly zabezpečení SSL a TLS v produktu IBM MQ” na stránce 22

IBM 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 nespolečně spolupracují.

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 vrstevovány 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 MQ je k dispozici na adrese “Povolení specifikace CipherSpecs” na stránce 393.

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.

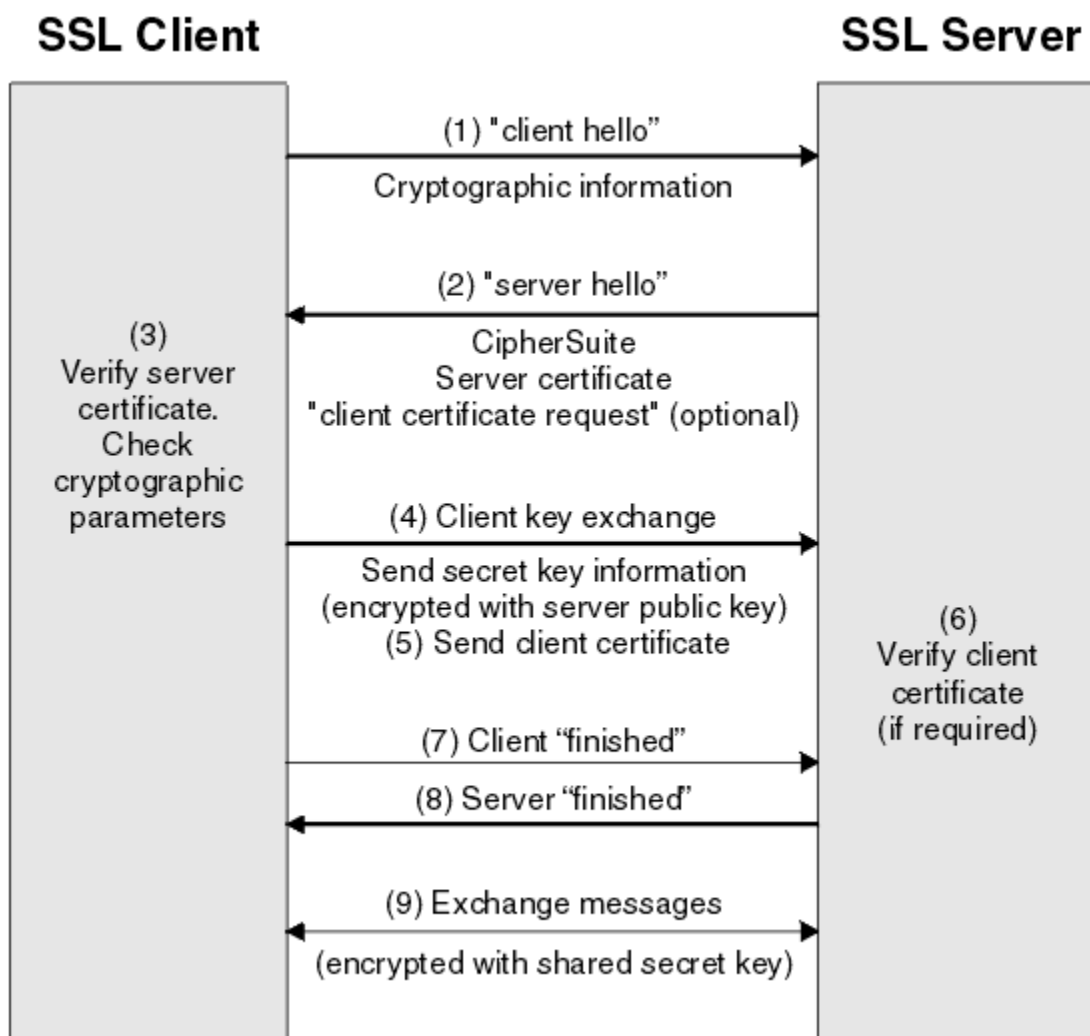
Další informace o šifrovacích algoritmech a digitálních certifikátech najdete v souvisejících informacích.

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 viz ["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 viz ["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 dešifrování 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 19).
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 322).

## 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 vyjednáán, 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 403](#).

Použití SSL nebo TLS zajišťuje integritu dat za předpokladu, že CipherSpec ve vaší definici kanálu používá hašovací algoritmus, jak je popsáno v tabulce v [“Povolení specifikace CipherSpecs” na stránce 393](#).

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.

V produktu IBM MQ 8.0.0, opravná sada Fix Pack 9 podporuje produkt IBM MQ protokol TLSv1.2. Můžete však povolit zamítnutý CipherSpecs, pokud to potřebujete.

Informace o následujících tématech viz [“Hodnoty CipherSpec podporované v produktu IBM MQ” na stránce 37](#) :

- CipherSpecs podporované produktem IBM MQ
- Jak zpřístupníte zamítnuté SSLv3 a TLSv1.0 CipherSpecs

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

Další informace o CipherSpecs viz [“Povolení specifikace CipherSpecs” na stránce 393](#).

Sada CipherSuite je sada šifrovacích algoritmů používaných připojením TLS nebo SSL. 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

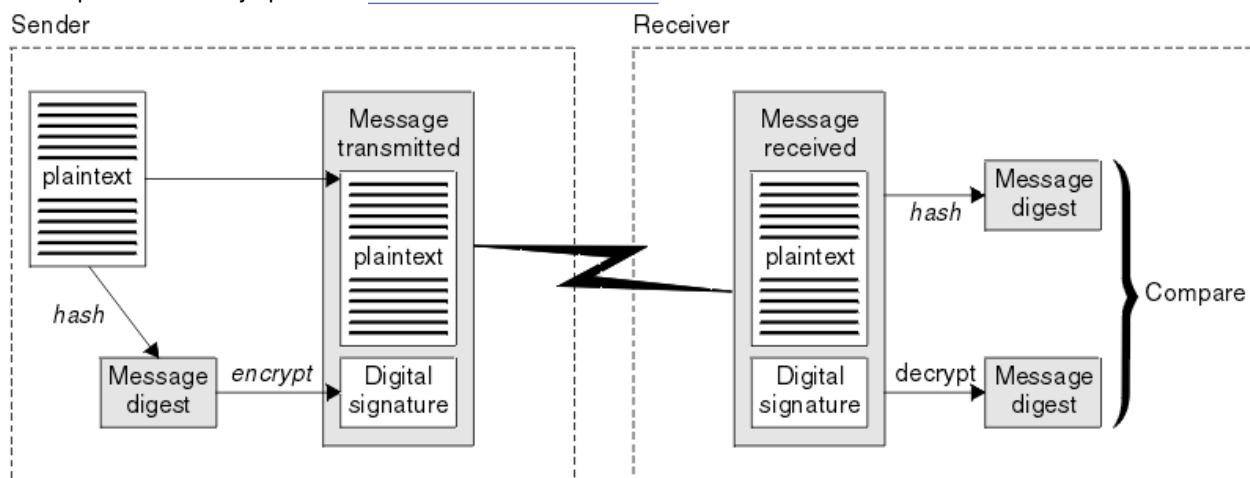
Digitální podpis je vytvořen šifrováním reprezentace zprávy. Šifrování používá soukromý klíč podepsané osoby a v zájmu efektivity obvykle pracuje na kódu digest zprávy spíše než na samotném zprávě.

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. Odesílatel 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 odesílatele.
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 odesílatel 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 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.

### **Související pojmy**

[“Národní bezpečnostní agentura \(NSA\) Suite B Kryptografie”](#) na stránce 20

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

### **Národní bezpečnostní agentura (NSA) Suite B Kryptografie**

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

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

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

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

1. Profil kompatibilní se sadou Suite B pro použití se TLS verze 1.2. Je-li konfigurována pro kompatibilní operaci Suite B, použije se pouze omezená sada šifrovacích algoritmů.
2. Přechnodný 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 přechnodnou operaci Suite B, mohou být použity další algoritmy šifrování a hašování.

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

Na systémech Windows, SYSTÉM UNIX a Linux, IBM MQ lze nakonfigurovat tak, aby vyhovovalo profilu TLS 1.2 standardu Suite B, ale nepodporuje přechnodný profil sady Suite B. Další informace uvádí téma [“Šifrování NSA Suite B v produktu IBM MQ”](#) na stránce 40.

### **Související odkazy**

[“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 MQ mechanismy zabezpečení**

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

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

### **Identifikace a ověření v produktu IBM MQ**

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

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

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

Informace o kontextu ve zprávě umožňují přijímající aplikaci zjistit informace o odesílateli zprávy. Obsahuje například název aplikace, která vložila tuto zprávu, a ID uživatele přidružené k aplikaci.

- Když se spustí kanál zpráv, je možné, aby byl agent kanálu zpráv (MCA) na každém konci kanálu autentizoval jeho partnera. Tato technika je známá jako *vzájemné ověření*. Pro odesílajícího agenta MCA poskytuje ujištění, že partner, o který se chystá odeslat zprávu, je původní. Pro přijímajícího agenta MCA existuje podobné ujištění o tom, že se chystá přijímat zprávu 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 MQ

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

Zde je několik příkladů autorizace v prostředí produktu IBM MQ :

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

Další informace o tom, jak nastavit autorizaci, najdete v tématu [“Plánování autorizace”](#) na stránce 71 a přidružených dílčích tématech.

### Související pojmy

“Autorizace” na stránce 6

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

## Auditování v IBM MQ

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

Zde je několik příkladů auditování v prostředí produktu IBM MQ :

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

### Související pojmy

“Auditování” na stránce 6

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

## Důvěrnost v IBM MQ

Důvěryhodnost v produktu IBM MQ můžete implementovat zašifrováním zpráv.

Utajení může být zajištěno v prostředí produktu IBM MQ takto:

- Jakmile odesílající agent MCA obdrží zprávu z přenosové fronty, produkt IBM MQ 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 mechanismy řízení přístupu poskytované produktem IBM MQ považovány za dostatečné pro ochranu jejich obsahu před neoprávněným zveřejněním. Avšak pro vyšší úroveň zabezpečení můžete použít produkt IBM MQ Advanced Message Security k šifrování zpráv uložených ve frontách.

### Související pojmy

[“Důvěrnost” na stránce 6](#)

Služba *confidentiality* chrání citlivé informace před neoprávněným zveřejněním.

## Integrita dat v produktu IBM MQ

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

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

- 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 MQ CipherSpecs poskytují algoritmus kódu digest zprávy, s výjimkou typu TLS\_RSA\_WITH\_NULL\_NULL, který neposkytuje integritu dat zprávy.

Produkt IBM MQ při příjmu zpráv zjišťuje změněné zprávy; při příjmu upravené zprávy příkaz IBM MQ vyvolá chybovou zprávu AMQ9661 a kanál se zastaví.

- Zatímco zprávy jsou uloženy v lokální frontě, mohou být mechanismy řízení přístupu poskytované produktem IBM MQ považovány za dostatečné pro zabránění záměrné úpravě obsahu zpráv.

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

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

### Související pojmy

[“Integrita dat” na stránce 7](#)

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

## Šifrování v produktu IBM MQ

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

Další informace viz [“Protokoly zabezpečení SSL a TLS v produktu IBM MQ” na stránce 22.](#)

### Související pojmy

[“Koncepte šifrování” na stránce 7](#)

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

## Protokoly zabezpečení SSL a TLS v produktu IBM MQ

IBM 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 IBM MQ podporuje verzi 3.0 protokolu SSL a verzi 1.0 a verzi 1.2 protokolu TLS. Můžete určit šifrovací algoritmy, které používá protokol SSL nebo protokol, zadáním hodnoty CipherSpec jako části definice kanálu.

**Poznámka:** **V 8.0.0.2** V produktu IBM MQ 8.0.0, opravná sada Fix Pack 2 je protokol SSLv3 a použití některých IBM MQ CipherSpecs zamítnuto. Další informace viz [Zamítnutí: Protokol SSLv3](#).

Můžete použít parametr [SECPROT](#) k zobrazení protokolu zabezpečení, který se používá na 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 IBM MQ na straně klienta kanálu MQI jedná jménem uživatele klientské aplikace IBM MQ. Během komunikace výměnou potvrzení protokolu SSL nebo TLS odesílá kód produktu IBM MQ digitální certifikát uživatele do agenta MCA na konci kanálu MQI kanálu MQI.

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

## Podpora pro SSL a TLS

Produkt IBM MQ poskytuje podporu pro SSL verze 3.0 a TLS 1.0 a TLS 1.2 podle platformy, kterou používáte. Další informace o protokolech SSL a TLS najdete v informacích v dílčích tématech.

### IBM i

Podpora zabezpečení SSL a TLS je integrální součástí operačního systému IBM i.

### Klienti Java a JMS

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

### Systémy HP Integrity NonStop Server, SYSTÉM UNIX, Linux a Okna

Podpora zabezpečení SSL a TLS je nainstalována s produktem IBM MQ.

### z/OS

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

Informace o předpokladech pro podporu SSL a TLS produktu IBM MQ naleznete v tématu [Systémové požadavky pro IBM MQ](#).

### 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 MQ podporuje zabezpečení SSL i TLS.

### Úložiště klíčů SSL nebo TLS

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

Tyto informace využívají obecný termín *úložiště klíčů* k popisování úložiště pro digitální certifikáty a jejich přidružené soukromé klíče. Úložiště klíčů je odkazováno různými názvy na různých platformách a prostředích, které podporují SSL a TLS:

-  V IBM i: *paměti certifikátů*
- V systémech Java a JMS: *keystore a truststore*
-    Na systémech SYSTÉM UNIX, Linuxu Okna : *key database file*
-  Na z/OS: *svazek klíčů*

Další informace naleznete v tématech [“digitální certifikáty”](#) na stránce 9 a [“Koncepte 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 následující certifikáty a požadavky:

- Řada certifikátů CA od různých certifikačních autorit, které umožňují správci front nebo klientovi ověřit certifikáty, které obdrží od svého partnera na vzdáleném konci připojení. Jednotlivé certifikáty mohou být v řetězu certifikátů.
- Jeden nebo více osobních certifikátů přijatých od certifikační autority. Ke každému správci front nebo IBM MQ MQI clientpřidružíte samostatný osobní certifikát. Osobní certifikáty jsou nezbytné pro klienta 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 úložiště klíčů IBM MQ”](#) na stránce 25.

Umístění úložiště klíčů závisí na platformě, kterou používáte:

#### IBM i

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

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

Paměť certifikátů také obsahuje soukromý klíč pro správce front.

#### Systémy SYSTÉM UNIX, Linuxu Okna

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

Každý soubor databáze klíčů má přidružený soubor pro uložení hesla. Tento soubor obsahuje kódovaná hesla, která umožňují programům přístup k databázi klíčů. Soubor pro uložení hesla musí být ve stejném adresáři a musí mít stejný soubor jako databáze klíčů a musí končit příponou .sth, například /var/mqm/qmgrs/QM1/ssl/key.sth

**Poznámka:** Šifrovací hardwarové karty PKCS #11 mohou obsahovat certifikáty a klíče, které jsou jinak uloženy v souboru databáze klíčů. Jsou-li certifikáty a klíče uchovávány na kartách PKCS #11, IBM MQ stále vyžaduje přístup k souboru databáze klíčů a k souboru pro uložení hesla.

V systémech UNIX a Windows obsahuje klíčová databáze také soukromý klíč pro osobní certifikát přidružený ke správci front nebo k produktu IBM MQ MQI client.

#### z/OS

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



Ostatní externí správci zabezpečení (ESM) také používají svazek klíčů pro ukládání certifikátů.

Soukromé klíče jsou spravovány produktem RACF.

### *Ochrana úložišť klíčů IBM MQ*

Úložiště klíčů pro IBM MQ je soubor. Ujistěte se, že má přístup k souboru úložiště klíčů pouze zamýšlený uživatel. Tím zabráníte tomu, aby narušitel nebo jiný neautorizovaný uživatel kopíroval soubor úložiště klíčů do jiného systému, a poté v systému, který má zosobňovat požadovaného uživatele, nastavení identického ID uživatele.

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

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

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

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

### *Digitální certifikáty certifikátu, základní informace o požadavcích*

Při nastavení 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.



## Co je jmenovka certifikátu?

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

Návěští certifikátu je oddělen od polí **Subject Distinguished Name** nebo **Subject Common Name** certifikátu. Všimněte si, že **Subject Distinguished Name** a **Subject Common Name** jsou pole v rámci certifikátu samotného. Ty jsou definovány při vytvoření certifikátu a nelze je změnit. Je-li to nezbytné, můžete změnit popisek přidružený k digitálnímu certifikátu.

## Syntaxe návěští certifikátu

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

-  Návěští certifikátu může obsahovat až 64 znaků.
-  Návěští certifikátu může obsahovat až 32 znaků.
- Návěští certifikátu nemůže obsahovat mezery.
- Štítky rozlišují velikost písmen.
- V systémech, které používají EBCDIC katakana, nemůžete používat malá písmena.
- Klient produktu IBM MQ pro štítky certifikátu produktu HP Integrity NonStop Server nesmí obsahovat dopředné lomítko (/), zpětné lomítko (\), tilda (lomítko), dolar (\$) nebo více než jedno po sobě jdoucí období (.)

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

## Jak se používá jmenovka certifikátu?

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

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

#### Notes:

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

V tomto kontextu odkazuje klient protokolu SSL nebo TLS k partnerovi připojení zahajujícímu navázání komunikace, což může být klient produktu IBM 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 MQ server SSL nebo TLS vždy požaduje certifikát od klienta a klient vždy poskytuje certifikát serveru, pokud je nalezen. Pokud klient nemůže najít osobní certifikát, pošle klientovi odpověď no certificate na server.

Server 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 *POVINNÍ* nebo nastaveným na hodnotu parametru **SSLPEER** .

Všimněte si, že příchozí kanály (včetně přijímačů, příjemců klastru, nekvalifikovaného serveru a kanálu připojení serveru) odesílají pouze nakonfigurovaný certifikát, pokud verze IBM MQ vzdáleného peeru plně podporuje konfiguraci jmenovek certifikátu a kanál používá TLS CipherSpec.

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

- Všechny aktuální klienty Java a JMS .
- Verze produktu IBM MQ před verzí Verze 8.0.

Kromě toho musí být certifikát použitý pro kanál vhodný pro kanál CipherSpec -další informace naleznete v dokumentu [“Digitální certifikáty a kompatibilita CipherSpec v produktu IBM MQ”](#) na stránce 44 .

Produkt IBM MQ 8.0 podporuje použití více certifikátů ve stejném správci front s použitím atributu štítku certifikátu na kanál. Příchozí kanály správce front (například připojení k serveru nebo příjemce) se spoléhají na zjištění názvu kanálu pomocí protokolu SNI (TLS Server Name Indication), aby mohl předložit správný certifikát od správce front.

Pokud používáte objekt MQIPT s přenosovou cestou, která má nastaveny obě volby *SSLServer* i *SSLClient* , existují mezi koncovými body dvě samostatné relace TLS a data SNI neprojdou přes přerušení relace.

Jednotlivé přenosové cesty MQIPT můžete použít k získání více podpory certifikátů výběrem příslušného certifikátu, například pomocí vlastností přenosové cesty *SSLServerSiteLabel* a *SSLClientSiteLabel* . Případně použijte příkaz MQIPT *SSLProxyMode* , který předává všechny řídicí toky SSL nebo TLS beze změny, včetně názvu SNI.

Všimněte si, že více certifikátů v rámci operace MQIPT funguje pouze v případě, že používáte režim serveru proxy SSL nebo TLS.

Další informace najdete v sekci podpory SSL/TLS v dokumentaci *IBM MQ Internet Pass-Thru* .

Další informace o připojení správce front s použitím jednosměrného ověření, tj. když klient SSL nebo TLS neodešle certifikát, najdete v tématu [Připojení dvou správců front s použitím jednosměrného ověření](#).

## IBM i, systémy SYSTEM UNIX, Linuxa Okna

 Server SSL nebo TLS odešle certifikát klientovi.

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

### Správci front

1. Atribut štítku certifikátu kanálu **CERTLABL**.
2. Atribut štítku certifikátu správce front **CERTLABL**.
3. Výchozí hodnota, která je ve formátu: `ibmwebspheremq` s připojeným názvem správce front, všechny malými písmeny. Například pro správce front s názvem QM1 je výchozí jmenovka certifikátu `ibmwebspheremqm1`.

### IBM MQ klienti

1. Atribut popisku certifikátu **CERTLABL** v definici kanálu CLNTCONN.
2. Struktura struktury MQSCO **CertificateLabel**.
3. Proměnná prostředí **MQCERTLABL**.
4. Client .ini file (in its SSL section) **CertificateLabel** attribute
5. Předvolba, která je ve formátu: `ibmwebspheremq` s ID uživatele, ke kterému je aplikace klienta spuštěna jako připojená, a to vše malými písmeny. Například pro ID uživatele produktu USER1 je výchozí popis certifikátu `ibmwebspheremquser1`.

### z/OS



IBM MQ Klienti nejsou na systémech z/OS podporováni. Správce front produktu z/OS však může při přijetí požadavku na připojení vystupovat v roli klienta SSL nebo TLS při inicializaci připojení nebo serveru zabezpečení SSL nebo TLS. Požadavky na štítky certifikátu pro správce front produktu z/OS se používají v obou těchto rolích a liší se od požadavků na distribuovaných platformách.

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

1. Atribut štítku certifikátu kanálu, **CERTLABL**.
2. Je-li sdílený, atribut návěští certifikátu skupiny sdílení front **CERTQSGL**.  
Pokud není sdílený, atribut návěští certifikátu správce front **CERTLABL**.
3. Výchozí hodnota, která je ve formátu: `ibmWebSphereMQ` s připojeným názvem správce front nebo skupiny sdílení front. Všimněte si, že tento řetězec rozlišuje velikost písmen a musí být zapsán tak, jak je zobrazen. Například pro správce front s názvem QM1 je výchozí jmenovka certifikátu `ibmWebSphereMQQM1`.
4. Pokud není nalezen certifikát s formátem ve volbě "3" na stránce 27, IBM MQ se pokusí použít certifikát označený jako výchozí v souboru svazku klíčů.

Informace o tom, jak zobrazit úložiště klíčů, viz ["Vyhledání úložiště klíčů pro správce front v systému z/OS"](#) na stránce 306.

### Klienti IBM MQ Java a IBM MQ JMS

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

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

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

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

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

## Klient IBM MQ pro HP Integrity NonStop Server

Klient IBM MQ pro HP Integrity NonStop Server používá atribut kanálu **CERTLABL** (nebo hodnotu proměnné prostředí **MQCERTLABL**) k výběru certifikátu, který má být použit pro připojení SSL.

Návěští certifikátu, ať už pochází z atributu **CERTLABL** kanálu nebo z hodnoty proměnné prostředí **MQCERTLABL**, se používá k vytvoření názvu souboru `cert*.pem` a odpovídajícího souboru `Stash*.sth`.

```
cert_<CERTLABL>.pem
Stash_<CERTLABL>.sth
```

Pokud kanál nemá atribut **CERTLABL** a proměnná prostředí **MQCERTLABL** není přítomna, pak IBM MQ použije následující certifikát a soubory pro uložení:

```
cert_default_<userid>.pem
Stash_default_<userid>.sth
```

kde `<userid>` je jméno uživatele, který spouští klientský program IBM MQ.

Pokud soubor `cert_default_<userid>.pem` nebo soubor `Stash_default_<userid>.sth` neexistuje, pak IBM MQ použije následující certifikát a soubory pro uložení:

```
cert.pem
Stash.sth
```

### Notes:

1. Náhradní řešení souborů `cert_default_<userid>.pem` a `Stash_default_<userid>.sth` nebo nekvalifikovaných `cert.pem` a `Stash.sth` files se vyskytuje pouze v případě, že je popis certifikátu dostupný z atributu **CERTLABL** kanálu, ani z proměnné prostředí **MQCERTLABL**. Je-li zadán příznak **CERTLABL**, musí existovat přidružené soubory `cert_<label>.pem` a `Stash_<label>.sth` a musí být přístupné pro pokračování v připojení.
2. IBM MQ odmítá nálepky na certifikáty obsahující některý z následujících znaků:

```
/
\  
~
$
```

a také odmítne návěští certifikátu obsahující více než jednu po sobě jdoucí tečku (.)

3. Přijímající program kanálu potřebuje získat přístup k certifikátu s názvem štítku používaným pro správce front, který je nastavením QMGR CERTLABL.

Výchozí hodnota pro nastavení QMGR CERTLABL je `ibmwebspheremq`, která je připojena k názvu správce front, a to vše malými písmeny. Například se správcem front s názvem QM1 je výchozí jmenovka certifikátu `ibmwebspheremqm1`

Toto pravidlo platí i v případě, že používáte atribut CERTLABL na kanálu k tomu, aby správci front sdělili, že má pro daný kanál použít jiný certifikát.

#### *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 IBM MQ . Další informace naleznete v tématu [Příkaz MQCMD\\_REFRESH\\_SECURITY](#) a v tématu *Aktualizace zabezpečení SSL nebo TLS* v části Průzkumník produktu IBM MQ v této dokumentaci produktu.

#### **Související pojmy**

“Aktualizace pohledu klienta na obsah úložiště klíčů SSL a nastavení zabezpečení SSL” na stránce 29  
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.

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

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

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

#### **Související pojmy**

“Aktualizace úložiště klíčů správce front” na stránce 29

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

#### **Ochrana heslem MQCSP**

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

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

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

Další informace o struktuře MQCSP naleznete v tématu [Struktura MQCSP](#).

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

- Oba konce připojení používají produkt IBM MQ 8.0 nebo novější.
- Kanál nepoužívá šifrování TLS. Kanál nepoužívá šifrování TLS, pokud má kanál prázdný atribut **SSLCIPH** , nebo je atribut **SSLCIPH** nastaven na hodnotu CipherSpec , která šifrování neposkytuje. Šifry NULL, například NULL\_SHA, nezajišťují šifrování.

- Nastavili jste **MQCSP.AuthenticationType** pro MQCSP\_AUTH\_USER\_ID\_AND\_PWD. Nastavení této hodnoty umožní vyhodnocení dalších kontrol při rozhodování o tom, zda je ochrana pomocí hesla provedena. Výchozí hodnota je **MQCSP.AuthenticationType** je MQCSP\_AUTH\_NONE. Při výchozím nastavení není ochrana heslem provedena. Další informace viz **AuthenticationType**.
- Pokud je klient IBM MQ Explorer a režim kompatibility identifikace uživatele není povolen, což není výchozí nastavení. Tato podmínka je použitelná pouze pro Průzkumníka IBM MQ .

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

## Nastavení konfigurace produktu PasswordProtection

Atribut **PasswordProtection** v sekci Channels v konfiguračním souboru klienta a souboru INI správce front může zabránit odesílání hesel v prostém textu. Atribut může mít 1 ze 3 hodnot. Předvolená hodnota je compatible:

### Kompatibilní

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

Proto:

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

### Vždy

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

Proto:

- Heslo je odesláno zašifrováno pomocí TLS CipherSpec , je-li použito šifrování TLS a CipherSpec nemá hodnotu null.
- Heslo je chráněno, pokud správce front i klient spouští verzi produktu IBM MQ na serveru Verze 8.0 nebo později, a nepoužívá se šifrování TLS, nebo je použita hodnota CipherSpec s hodnotou null. **MQCSP**Hodnota **AuthenticationType** musí být nastavena na hodnotu MQCSP\_AUTH\_USER\_ID\_AND\_PWD.
- Připojení selže před odesláním hesla, pokud správce front nebo klient spouští verzi produktu IBM MQ starší než verze Verze 8.0a šifrování TLS se nepoužívá. Vzhledem k tomu, že verze produktu IBM MQ starší než Verze 8.0 mohou odesílat hesla pouze v prostém textu a produkt a1ways vyžaduje, aby bylo heslo buď šifrováno, nebo chráněno, připojení selže.

### volitelné

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

Proto:

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

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

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

Další informace o ověření připojení s klienty Java a JMS viz [“Ověření spojení s klientem Java”](#) na stránce 65.

### ***Správce digitálních certifikátů (DCM)***

Použijte produkt DCM ke správě digitálních certifikátů a soukromých klíčů na IBM i.

Produkt DCM (Digital Certificate Manager vám umožňuje spravovat digitální certifikáty a používat je v zabezpečených aplikacích na serveru IBM i . Pomocí produktu Digital Certificate Manager můžete požadovat a zpracovat digitální certifikáty od certifikačních autorit (CA) nebo jiných třetích stran. Pro vytvoření a správu digitálních certifikátů pro své uživatele můžete také sloužit jako lokální vydavatel certifikátů.

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

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

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

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

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

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




## **Federální standardy zpracování informací (FIPS)**

Toto téma představuje program pro ověření standardu FIPS (Federal Information Processing Standards) programu US National Institute of Standards and Technology a kryptografické funkce, které lze použít na kanálech SSL nebo TLS.

Tyto informace se vztahují na následující platformy:

- Windows
- SYSTÉM UNIX a Linux
- z/OS

Shoda se standardem FIPS 140-2 na IBM MQ zabezpečení SSL nebo TLS na systémech SYSTÉM UNIX, Linuxu a Okna se nachází zde [“Federální standardy zpracování informací \(FIPS\) pro SYSTÉM UNIX, Linuxu a Okna”](#) na stránce 32.

 Shoda s FIPS 140-2 připojení IBM MQ SSL nebo TLS na z/OS se nachází zde [“Federální standardy zpracování informací \(FIPS\) pro z/OS”](#) na stránce 35.

Je-li přítomen kryptografický hardware, mohou být kryptografické moduly používané produktem IBM 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 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 255

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

[“Použití runmqckm, runmqakm a strmqikm pro správu digitálních certifikátů”](#) na stránce 274

V systémech UNIX, Linux a Windows spravujte klíče a digitální certifikáty pomocí **strmqikm** (iKeyman). GUI, nebo z příkazového řádku pomocí **runmqckm** (iKeycmd) nebo **runmqakm** (GSKCapiCmd).

### **Související odkazy**

[“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).

### **Související informace**

[Povolení zabezpečení SSL v produktu IBM MQ classes for Java](#)

[Vlastnosti SSL pro objekty produktu JMS](#)

[Použití SSL \(Secure Sockets Layer\) s IBM MQ classes for JMS](#)

*Federální standardy zpracování informací (FIPS) pro SYSTÉM UNIX, Linuxu a Okna*

When cryptography is required on an SSL/TLS channel on Windows, SYSTÉM UNIX a Linux systems, IBM MQ uses a cryptography package called IBM Crypto for C (ICC). Na platformách Windows, SYSTÉM UNIX a Linux, schválil software ICC standardy FIPS (Federal Information Processing Standards) programu US National Institute of Standards and Technology (Federal Information Processing Standards) na úrovni 140-2.

Shoda s FIPS 140-2 připojení IBM MQ TLS na Windows, SYSTÉM UNIX a Linux systémy je následující:

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



- Instalovaná verze GSKit ICC byla certifikována FIPS 140-kompatibilní s verzí instalovaného operačního systému a s architekturou hardwaru.
- Atribut SSLFIPS správce front byl nastaven na hodnotu YES.
- Všechna úložiště klíčů byla vytvořena a manipulována pomocí softwaru kompatibilního se standardem FIPS, jako je například **runmqakm** s volbou `-fips`.
- Pro všechny aplikace produktu IBM MQ MQI client používá připojení sadu GSKit a je kompatibilní se standardem FIPS, jsou-li splněny následující podmínky:
  - Instalovaná verze GSKit ICC byla certifikována FIPS 140-kompatibilní s verzí instalovaného operačního systému a s architekturou hardwaru.
  - Zadali 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 manipulována pomocí softwaru kompatibilního se standardem FIPS, jako je například **runmqakm** s volbou `-fips`.
- Pro aplikace produktu IBM MQ classes for Java používající režim klienta používá toto připojení implementace TLS prostředí JRE a je kompatibilní se standardem FIPS, jsou-li splněny následující podmínky:
  - Běhové prostředí produktu Java použité ke spuštění aplikace je kompatibilní se standardem FIPS na instalované verzi operačního systému a architektuře hardwaru.
  - Zadali jste, že má být použito pouze šifrování s certifikací FIPS, jak je popsáno v souvisejícím tématu pro klienta Java.
  - Všechna úložiště klíčů byla vytvořena a manipulována pomocí softwaru kompatibilního se standardem FIPS, jako je například **runmqakm** s volbou `-fips`.
- Pro aplikace produktu IBM MQ classes for JMS používající režim klienta používá toto připojení implementace TLS prostředí JRE a je kompatibilní se standardem FIPS, jsou-li splněny následující podmínky:
  - Běhové prostředí produktu Java použité ke spuštění aplikace je kompatibilní se standardem FIPS na instalované verzi operačního systému a architektuře hardwaru.
  - Zadali jste, že má být použito pouze šifrování s certifikací FIPS, jak je popsáno v souvisejícím tématu pro klienta JMS.
  - Všechna úložiště klíčů byla vytvořena a manipulována pomocí softwaru kompatibilního se standardem FIPS, jako je například **runmqakm** s volbou `-fips`.
- V případě nespravovaných aplikací klienta .NET používá připojení sadu GSKit a vyhovuje FIPS, jsou-li splněny následující podmínky:
  - Instalovaná verze GSKit ICC byla certifikována FIPS 140-kompatibilní s verzí instalovaného operačního systému a s architekturou hardwaru.
  - Zadali jste, že má být použito pouze šifrování s certifikací FIPS, jak je popsáno v souvisejícím tématu pro klienta .NET.
  - Všechna úložiště klíčů byla vytvořena a manipulována pomocí softwaru kompatibilního se standardem FIPS, jako je například **runmqakm** s volbou `-fips`.
- Pro nespravované aplikace klienta XMS .NET používá připojení sadu GSKit a je kompatibilní se standardem FIPS, jsou-li splněny následující podmínky:
  - Instalovaná verze GSKit ICC byla certifikována FIPS 140-kompatibilní s verzí instalovaného operačního systému a s architekturou hardwaru.
  - Zadali jste, že má být použito pouze šifrování s certifikací FIPS, jak je popsáno v dokumentaci k produktu XMS .NET.
  - Všechna úložiště klíčů byla vytvořena a manipulována pomocí softwaru kompatibilního se standardem FIPS, jako je například **runmqakm** s volbou `-fips`.

Všechny podporované platformy jsou certifikovány FIPS 140-2 s výjimkou těch, které jsou uvedeny v souboru Readme, který je součástí každé opravné sady nebo aktualizacího balíku.

Pro připojení TLS využívající GSKit má komponenta, která je certifikovaná FIPS 140-2, název ICC. Jedná se o verzi této komponenty, která určuje shodu GSKit FIPS na libovolné dané platformě. Chcete-li zjistit momentálně nainstalovanou verzi ICC, spusťte příkaz **dspmqver -p 64 -v**.

Zde je příklad výpisu výstupu příkazu **dspmqver -p 64 -v** týkající se ICC:

```
ICC
=====
@ (#)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, 2023.
@ (#) Všechna práva vyhrazena. Uživatelé vládních institucí USA
@ (#) Omezená práva-Použití, duplikace nebo vyzrazení
@ (#) je omezeno smlouvou GSA ADP Schedule Contract with 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:
```

Certifikační příkaz NIST pro sadu GSKit ICC 8 (obsažený v sadě GSKit 8) lze nalézt na následující adrese: [Cryptographic Module Validation Program](#).

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

## Při práci v souladu s FIPS 140-2 jsou vynucována omezení Triple DES

Je-li produkt IBM MQ nakonfigurován tak, aby pracoval v souladu se standardem FIPS 140-2, jsou ve vztahu ke Triple DES (3DES) CipherSpecs vynucována další omezení. Tato omezení umožňují shodu s doporučením americké NIST SP800-67.

1. Všechny části klíče Triple DES musí být jedinečné.
2. Žádná část klíče Triple DES nemůže být Slabá, Semi-Slabá nebo možná-Slabá klávesa podle definice v NIST SP800-67.
3. Více než 32 GB dat může být přeneseno přes připojení před tím, než se musí provést reset tajného klíče. Ve výchozím nastavení IBM MQ neobnoví tajný klíč relace, takže musí být tento reset nastaven. Selhání při povolení resetování tajného klíče při použití výsledků slučitelnosti Triple DES CipherSpec a FIPS 140-2 při zavírání připojení s chybou AMQ9288 po překročení maximálního počtu bajtů. Informace o tom, jak nakonfigurovat resetování tajného klíče, viz [“Resetování tajných klíčů SSL a TLS” na stránce 400](#).

IBM MQ generuje klíče relací Triple DES, které již jsou v souladu s pravidly 1 a 2. Chcete-li však splnit třetí omezení, musíte povolit reset tajného klíče, když používáte konfiguraci Triple DES CipherSpecs v konfiguraci FIPS 140-2. Případně se můžete vyhnout použití Triple DES.

### Související pojmy

[“Určení, že pro běhové prostředí klienta MQI je použit pouze certifikovaný standard FIPS CipherSpecs” na stránce 255](#)

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

[“Použití runmqckm, runmqakm a strmqikm pro správu digitálních certifikátů” na stránce 274](#)

V systémech UNIX, Linux a Windows spravujte klíče a digitální certifikáty pomocí **strmqikm** (iKeyman). GUI, nebo z příkazového řádku pomocí **runmqckm** (iKeycmd) nebo **runmqakm** (GSKCapiCmd).

## Související odkazy

“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).

## Související informace

[Povolení zabezpečení TLS v produktu IBM MQ classes for Java](#)

[Vlastnosti TLS pro objekty JMS](#)

[Použití protokolu TLS \(Transport Layer Security\) s produktem IBM MQ classes for JMS](#)

### *Federální standardy zpracování informací (FIPS) pro z/OS*

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

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

- Chcete-li povolit kanály zpráv produktu IBM MQ pro prostředí FIPS-slučitelnost, ujistěte se, že jsou splněny následující podmínky:
  - Produkt System SSL Security Level 3 FMID je instalován a konfigurován (viz [Plánování instalace produktu IBM MQ](#)).
  - Systémové moduly SSL jsou ověřovány.
  - Atribut SSLFIPS správce front byl nastaven na hodnotu **YES**.

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

algoritmus	Ne-FIPS		FIPS	
	Velikosti klíče	Hardware	Velikosti klíče	Hardware
RC2	40 a 128			
RC4	40 a 128			
DES	56	x		
TDES	168	x	168	x
AES	128 a 256	x	128 a 256	x
MD5	48			
SHA-1	160	x	160	x
SHA-2	224, 256, 384 a 512	x	224, 256, 384 a 512	x
RSA	512-4096	x	1024-4096	x
DSA	512-1024		1024	
DH	512-2048		2048	

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

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

Informace o konfiguraci System SSL naleznete v tématu [Nastavení ověření modulu systémového zabezpečení SSL](#).

### **Související odkazy**

[“Federální standardy zpracování informací” na stránce 19](#)

Americká vláda poskytuje technické poradenství v oblasti IT systémů a 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 na serveru IBM MQ MQI client**

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

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

Úložiště klíčů pro IBM MQ MQI client můžete určit buď pomocí hodnoty MQSSLKEYR v konfiguračním souboru klienta IBM MQ, nebo při volání aplikace MQCONN. Existují tři možnosti určení, že kanál používá zabezpečení SSL:

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

Pomocí proměnné prostředí MQSERVER nelze určit, že kanál používá zabezpečení SSL.

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

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 projevíly 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.

Když se IBM MQ MQI client spustí na systému Windows, SYSTÉM UNIX a Linux se šifrovacím hardwarem, nakonfigurujte hardware s proměnnou prostředí MQSSLCRYP. Tato proměnná je ekvivalentní parametru SSLCRYP v příkazu ALTER QMGR MQSC. Popis parametru SSLCRYP v příkazu ALTER QMGR MQSC najdete v tématu [ALTER QMGR](#) (popis parametru SSLCRYP). Pokud použijete verzi parametru SSLCRYP GSK\_PCS11, musí být popisek tokenu PKCS #11 určen zcela v menším případě.

Resetování tajných klíčů SSL a FIPS jsou podporovány na IBM MQ MQI clients. Další informace naleznete v tématech [“Resetování tajných klíčů SSL a TLS” na stránce 400](#) a [“Federální standardy zpracování informací \(FIPS\) pro SYSTÉM UNIX, Linux a Okna” na stránce 32](#).

Další informace o podpoře SSL pro produkt IBM MQ MQI clients viz [“Nastavení zabezpečení produktu IBM MQ MQI client” na stránce 254](#).

### **Související informace**

[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 MQ na platformě klienta.

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

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

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

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

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 MQCONN.

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

Jedna nebo více položek v tabulce definic kanálů klienta může určovat název CipherSpec. Pokud například vytvoříte položku pomocí příkazu DEFINE CHANNEL MQSC, můžete použít parametr SSLCIPH v příkazu k určení názvu CipherSpec.

4. Použití Active Directory na systému Windows.

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

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

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 CipherSpec pro IBM MQ MQI client” na stránce 399](#)

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

### **CipherSpecs a CipherSuites v produktu IBM MQ**

V produktu IBM MQ 8.0.0, opravná sada Fix Pack 9 podporuje produkt IBM MQ TLS V1.2 CipherSpecs algoritmy RSA a Diffie-Hellman. Můžete však povolit zamítnutý CipherSpecs, pokud to potřebujete.

Informace o následujících tématech viz [“Hodnoty CipherSpec podporované v produktu IBM MQ” na stránce 37](#) :

- CipherSpecs podporované produktem IBM MQ
- Jak povolit zamítnuté CipherSpecs

Produkt IBM MQ podporuje algoritmus výměny klíčů RSA a Diffie-Hellman a ověřovací algoritmy. Velikost klíče použitého během TSL nebo handshake 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.

### **V 8.0.0.3 Hodnoty CipherSpec podporované v produktu IBM 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

 Výchozí sada CipherSpecs pro produkt IBM MQ for IBM i verze 7.2 a verze 7.3 povoluje pouze následující hodnoty:

- \*TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- \*TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- \*ECDHE\_ECDSA\_RC4\_128\_SHA256
- \*ECDHE\_RSA\_RC4\_128\_SHA256
- \*ECDHE\_RSA\_3DES\_EDE\_CBC\_SHA256
- \*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
- \*ECDHE\_RSA\_NULL\_SHA256
- \*ECDHE\_ECDSA\_NULL\_SHA256

## Povolení zamítnuté TLS CipherSpecs

Ve výchozím nastavení není povoleno určit zamítnutou položku CipherSpec v definici kanálu. Pokud se pokusíte zadat zamítnutou položku CipherSpec, obdržíte zprávu AMQ8242: Chybná definice SSLCIPH a PCF vrátí hodnotu MQRCCF\_SSL\_CIPHER\_SPEC\_ERROR.

Nemůžete spustit kanál se zamítnutou volbou CipherSpec. Pokud se pokusíte tak učinit se zamítnutým CipherSpec, systém vrátí *MQCC\_FAILED (2)* spolu s **Reason** *MQRCC\_SSL\_INITIALIZATION\_ERROR (2393)* na klienta.

Je možné, abyste znovu povolili jednu nebo více zamítnutých CipherSpecs pro definování kanálů za běhu na serveru nastavením proměnné prostředí *AMQ\_SSL\_WEAK\_CIPHER\_ENABLE*.

Proměnná prostředí `AMQ_SSL_WEAK_CIPHER_ENABLE` přijímá:

- jeden název CipherSpec , nebo
- Čárkami oddělený seznam názvů IBM MQ CipherSpec , které mají být znovu povoleny, nebo
- Speciální hodnota `ALL` představující všechny CipherSpecs.

Chcete-li například znovu povolit `ECDHE_RSA_RC4_128_SHA256`, nastavte tuto proměnnou prostředí:

```
AMQ_SSL_WEAK_CIPHER_ENABLE=ECDHE_RA_RC4_128_SHA256
```

nebo alternativně změnit sekci SSL v souboru `qm.ini` nastavením:

```
SSL
AllowWeakCipherSpec=ECDHE_RA_RC4_128_SHA256
```

## Povolení zamítnutého SSL CipherSpecs

Kromě vydání `AMQ_SSL_WEAK_CIPHER_ENABLE` nebo `AllowWeakCipherSpec`, jak je popsáno v “Povolení zamítnuté TLS CipherSpecs” na stránce 38, musíte nastavit proměnnou prostředí `AMQ_SSL_V3_ENABLE=1` nebo vydat příkaz `AllowSSLV3=Y`, jak je popsáno v části [Deprecation:SSLV3 protokol](#).

Chcete-li například znovu povolit `RC4_MD5_US`, nastavte následující proměnné prostředí:

```
AMQ_SSL_V3_ENABLE=1
AMQ_SSL_WEAK_CIPHER_ENABLE=RC4_MD5_US
```

nebo alternativně změňte oddíl SSL v souboru `qm.ini` nastavením:

```
SSL
AllowSSLV3=Y
AllowWeakCipherSpec=RC4_MD5_US
```



**Upozornění:** Následující informace týkající se `TLS_V1` se týkají pouze produktu IBM MQ 8.0.0, opravná sada Fix Pack 9 .

Kromě vydání `AMQ_TLS_WEAK_CIPHER_ENABLE` nebo `AllowWeakCipherSpec` musíte nastavit proměnnou prostředí `AMQ_TLS_V1_ENABLE=1` nebo nastavit `AllowTLV1=Y`, chcete-li pokračovat v používání zamítnutého serveru `TLSv1 CipherSpecs`.

Chcete-li například znovu povolit `TLS_RSA_WITH_AES_128_CBC_SHA`, nastavte následující proměnné prostředí:

```
AMQ_TLS_V1_ENABLE=1
AMQ_TLS_WEAK_CIPHER_ENABLE=TLS_RSA_WITH_AES_128_CBC_SHA
```

nebo alternativně změňte oddíl SSL v souboru `qm.ini` nastavením:

```
SSL
AllowTLV1=Y
AllowWeakCipherSpec=TLS_RSA_WITH_AES_128_CBC_SHA
```

## Povolení zamítnutých CipherSpecs na serveru z/OS



Ve výchozím nastavení není povoleno určit zamítnutou položku CipherSpec v definici kanálu. Pokud se o uvedení zamítnuté položky CipherSpec v systému z/OS, obdržíte zprávu `CSQM102E` nebo zprávu `CSQX674E`.



Chcete-li povolit slabé (zastaralé) šifrovací specifikace, musíte definovat následující příkaz DD v souboru CHINIT JCL:

```
//DD CSQXWEAK DUMMY
```

Chcete-li povolit zamítnutý protokol SSLv3 , musíte také definovat následující příkaz DD v souboru CHINIT JCL:

```
//DD CSQXSSL3 DUMMY
```

Chcete-li povolit zamítnutý protokol TLSv1 , musíte také definovat následující příkaz DD v souboru CHINIT JCL:

```
//DD CSQXTLS1 DUMMY
```

### 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 MQ

Toto téma poskytuje informace o tom, jak nakonfigurovat produkt IBM MQ na systémech Windows, Linuxu UNIX , aby vyhověli 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 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 7.5 uvádí verzi sady Suite B, která je vynucována jednotlivými úrovněmi údržby produktu. Pokud nakonfigurujete produkt IBM MQ pro vynucení shody Suite B, vždy při plánování použití údržby konzultujte soubor Readme.

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

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 <sup>1</sup>	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 MQ není v souladu se standardem Suite B, produkt IBM MQ může být nakonfigurován tak, aby vyhovoval oběma úrovním zabezpečení v systémech Windows, SYSTÉM UNIX a Linux . Po úspěšné konfiguraci produktu IBM 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\_B klientem 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 IBM MQ CipherSpecs viz [“Povolení specifikace CipherSpecs”](#) na stránce 393

## 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 IBM MQ nakonfigurován tak, aby používal certifikáty, jejichž digitální podpisový algoritmus a typ veřejného klíče je povolen na konfigurované úrovni 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:** Příkazy **runmqckm** a **strmqikm** nepodporují vytváření digitálních certifikátů pro kompatibilní operaci Suite B.

## Vytvoření a vyžádání digitálních certifikátů

Chcete-li vytvořit samopodepsaný digitální certifikát pro testování Suite B, prohlédněte si téma [“Vytvoření osobního certifikátu podepsaného sebou samým na serveru SYSTÉM UNIX, Linuxa Okna”](#) na stránce 281

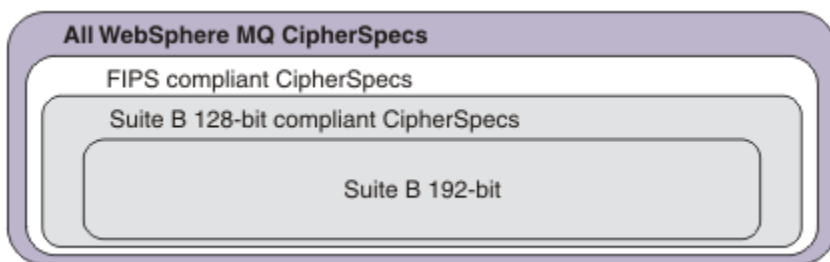
Chcete-li požádat o digitální certifikát podepsaný CA pro provozní použití Suite B, prohlédněte si téma [“Požádání o osobní certifikát v systému SYSTÉM UNIX, Linuxa Okna”](#) na stránce 284.

**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 MQ nakonfigurováno pro operaci vyhovující FIPS 140-2. Proto je možné nakonfigurovat IBM MQ jak pro standard FIPS, tak pro sadu Suite B současně, v tom případě se použijí obě sady omezení.

Následující diagram ilustruje vztah mezi těmito dílčími sadami:



## Konfigurace produktu IBM MQ pro kompatibilní operaci Suite B

Informace o tom, jak nakonfigurovat produkt IBM MQ v systému Windows, SYSTÉM UNIX a Linux pro provoz standardu Suite B naleznete v tématu [“Konfigurace produktu IBM MQ pro sadu Suite B”](#) na stránce 42.

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

### Související pojmy

[“Určení, že pro běhové prostředí klienta MQI je použit pouze certifikovaný standard FIPS CipherSpecs”](#) na stránce 255

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

## Konfigurace produktu IBM MQ pro sadu Suite B

Produkt IBM MQ může být nakonfigurován tak, aby pracoval v souladu se standardem NSA Suite B na platformách Windows, SYSTÉM UNIX a Linux .

Sada B omezuje sadu povolených šifrovacích algoritmů tak, aby byla zajištěna zajištěná úroveň zabezpečení. Produkt IBM MQ může být nakonfigurován tak, aby pracoval v souladu se sadou Suite B, který poskytuje rozšířenou úroveň zabezpečení. Další informace o Suite B najdete v tématu [“Národní bezpečnostní agentura \(NSA\) Suite B Kryptografie”](#) na stránce 20. 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 MQ”](#) na stránce 40.

## 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](#).

Ke konfiguraci správce front pro vyhovující operaci Suite B můžete také použít příkaz PCF **MQCMD\_CHANGE\_Q\_MGR** s parametrem **MQIA\_SUITE\_B\_STRENGTH** .

**Poznámka:** Pokud změníte nastavení Suite B správce front, je třeba restartovat službu MQXR, aby tato nastavení byla účinná.

## Klient MQI

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

1. Nastavením pole **EncryptionPolicySuiteB** ve struktuře MQSCO na volání MQCONNX se zobrazí jedna nebo více z následujících 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 MQSUIEB na jednu nebo více z následujících 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 následujících 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 MQSUIEB, 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 MQSUIEB naleznete v tématu [Proměnné prostředí](#).

## .NET

U nespravovaných klientů .NET je vlastnost **MQC.ENCRYPTION\_POLICY\_SUITE\_B** označuje typ zabezpečení Suite B, který je požadován.

Informace o použití Suite B v produktu IBM MQ classes for .NET najdete v tématu [Třída MQEnvironment .NET](#).

## AMQP

V 8.0.0.4

Nastavení atributu Suite B pro správce front se vztahuje na kanály AMQP v daném správci front. Pokud upravíte nastavení sady Suite B správce front, je třeba restartovat službu AMQP, aby se změny projevíly.

### **Zásady ověření platnosti certifikátu v produktu IBM MQ**

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

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

- Pro aplikace Java a JMS na všech platformách závisí zásada ověření platnosti certifikátu na komponentě JSSE běhového prostředí produktu Java . Další informace o zásadě ověření platnosti certifikátu naleznete v dokumentaci k vašemu prostředí JRE.
- Pro systémy IBM i závisí zásada ověření platnosti certifikátu na zabezpečené soketové knihovně poskytnuté operačním systémem. Další informace o zásadě ověření platnosti certifikátu naleznete v dokumentaci k operačnímu systému.
- Pro systémy z/OS závisí zásada ověření platnosti certifikátu na komponentě System SSL, kterou poskytuje operační systém. Další informace o zásadě ověření platnosti certifikátu naleznete v dokumentaci k operačnímu systému.
- Pro systémy SYSTÉM UNIX, Linux a Okna 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 SYSTÉM UNIX, Linuxu Okna , viz [“Konfigurace zásad ověření platnosti certifikátu v produktu IBM MQ”](#) na stránce 44. 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 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 MQ”](#) na stránce 43.

### **Digitální certifikáty a kompatibilita CipherSpec v produktu IBM 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 MQ.

Ve vydáních před produktem IBM WebSphere MQ 7.1 byly všechny podporované TLS CipherSpecs používány algoritmem 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 7.1 a novější 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 CipherSpec získat 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 CipherSpecs na základě protokolu TLS 1.2 , ujistěte se, že digitální certifikáty nepoužívají algoritmus MD5 ve svých digitálních podpisech. Starší CipherSpecs , které používají protokoly TLS 1.0 , se na toto omezení nevztahují 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 popis certifikátu algoritmu digitálního podpisu, který má být zobrazen. Podrobnosti najdete v tématu [Digitální certifikáty certifikátu](#) .

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

Spuštěním příkazu **runmqakm** se zobrazí výstup zobrazující použití zadaného podpisového algoritmu:

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

Řádek `Signature Algorithm` 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 CipherSpec označené předponou názvu CipherSpec . Každý typ CipherSpec klade různá omezení na typ digitálního certifikátu, který může být použit. Tato omezení platí pro všechna připojení IBM MQ TLS, ale jsou zvláště důležitá pro uživatele šifrování Elliptic Curve.

Následující tabulka shrnuje vztahy mezi CipherSpecs a digitálními certifikáty:

Tabulka 4. Vztahy mezi CipherSpecs a digitálními certifikáty

Typ	Předpona názvu CipherSpec	Popis	Požadovaný typ veřejného klíče	Algoritmus šifrování digitálních o 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 RSA.	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 nejsou správci front produktu IBM MQ a klienti MQI na platformě IBM i podporovány správci front a klienty MQI.

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.

Můžete nakonfigurovat kanál se sadou CipherSpec , která vyžaduje certifikát EC (Elliptic Curve), a popisek certifikátu pro certifikát RSA, nebo druhé kolo. Musíte se ujistit, že certifikát uvedený v označení certifikátu odpovídá pro kanál CipherSpec.

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

- Jednotlivý správce front se směsí certifikátů RSA a EC.
- Různé kanály ve stejném správci front s použitím certifikátu RSA nebo EC.

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 s MD5 nebo ECDSA s 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 IBM MQ nakonfigurován tak, aby vyhovoval standardům FIPS 140-2 nebo NSA Suite B, pak bude také omezen rozsah přípustných konfigurací. Další informace naleznete v následující sekci.

Pokud potřebujete použít různé typy CipherSpec ve stejném správci front nebo klientské aplikaci, konfiguruje příslušnou jmenovku certifikátu a kombinaci CipherSpec v definici klienta.

Tři typy CipherSpec nespolupracují přímo: jedná se o omezení aktuálních standardů TLS. Předpokládejme například, že jste zvolili použití 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 vzdálený odesílací konec kanálu TO.QM1 musí mít osobní certifikát s klíčem Elliptic Curve a digitálním podpisem na bázi ECDSA. Pokud vzdálený odesílací kanál nesplňuje tyto požadavky, kanál se nespustí.

Další kanály, které se připojují ke správci front QM1, mohou použít jiné CipherSpecs za předpokladu, že každý kanál používá certifikát správného typu pro CipherSpec daného kanálu. Předpokládejme například, že QM1 používá odesílací kanál s názvem TO.QM2 odešle zprávy do jiného správce front s názvem QM2. Kanál TO.QM2 by mohla použít typ 3 CipherSpec TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256, a to za předpokladu, že oba konce kanálu používají certifikáty obsahující veřejné klíče RSA. Atribut kanálu popisku certifikátu lze použít ke konfiguraci jiného certifikátu pro každý kanál.

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

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

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

kde *cert\_label* je popis certifikátu, jehož algoritmus digitálního podpisu je třeba zobrazit. Podrobnosti najdete v tématu [Digitální certifikáty certifikátu](#).

Spuštěním příkazu **runmqakm** se zobrazí výstup zobrazující typ veřejného klíče:

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



Řádek Typ veřejného klíče v tomto případě ukazuje, že certifikát má veřejný klíč Elliptic Curve. Řádek 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.

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

## Eliptická křivka CipherSpecs a NSA Suite B

Je-li produkt IBM 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 MQ”](#) na stránce 40. 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_SHA256` nebo `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:

<i>Tabulka 5. Podporované eliptické křivky NIST</i>		
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

[“Povolení specifikace CipherSpecs”](#) na stránce 393

Povolte CipherSpec pomocí parametru **SSLCPH** 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 255

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 MQ”](#) na stránce 40

Toto téma poskytuje informace o tom, jak nakonfigurovat produkt IBM MQ na systémech Windows, Linuxu UNIX, aby vyhověli profilu TLS 1.2 standardu Suite B.

[“Národní bezpečnostní agentura \(NSA\) Suite B Kryptografie”](#) na stránce 20

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

## Záznamy ověření kanálu

Chcete-li zlepšit kontrolu nad udílením přístupu k připojícím 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 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 spuštění 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**.

<i>Tabulka 6. Kde se použijí pravidla CHLAUTH pro různé dvojice kanálů</i>	
<b>Typ kanálu</b>	<b>MCA, kde jsou použita pravidla CHLAUTH</b>
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 IBM MQ. Tyto adresy musí být dočasně blokovány, dokud nedojde k aktualizaci brány firewall. Tyto pokusy o připojení ani nemůžou pocházet z kanálů produktu IBM MQ, ale z jiných soketových aplikací; které jsou nesprávně nakonfigurované pro zaměření vašeho modulu listener produktu IBM MQ. Adresy IP můžete blokovat nastavením záznamu ověřování kanálu typu BLOCKADDR. Můžete zadat jednu nebo více adres, rozsahy adres či vzorce zahrnující zástupné znaky.

Pokud dojde k odmítnutí příchozího připojení kvůli blokování adresy IP tímto způsobem, vydá se zpráva události MQRChannelBlocked s kvalifikátorem příčiny MQRChannelBlockedAddress, 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 MQRChannelBlocked s kvalifikátorem příčiny MQRChannelBlockedNoAccess, za předpokladu, že události kanálu jsou povoleny a správce front je spuštěný.

Příklad najdete v části [“Blokování určitých adres IP”](#) na stránce 362.

## 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 MQRChannelBlocked s kvalifikátorem příčiny MQRChannelBlockedUserID za předpokladu, že jsou povoleny události kanálu.

Příklad najdete v části [“Blokování specifických ID uživatelů”](#) na stránce 363.

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 MQRChannelBlocked s kvalifikátorem příčiny MQRChannelBlockedNoAccess, 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 366.

## 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 MQRChannelBlocked s kvalifikátorem příčiny MQRChannelBlockedNoAccess, za předpokladu, že události kanálu jsou povoleny a správce front je spuštěný.

Příklad najdete v části [“Blokování přístupu ze vzdáleného správce front”](#) na stránce 366.

## 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 přichozího připojení z této příčiny, vydá se zpráva události MQRQ\_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 367.

### **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 367.

### **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 364.

### **Mapování ID uživatelů deklarovaných klientem na používaná ID uživatele**

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

Příklad najdete v části [“Mapování uživatelem deklarovaného ID uživatele na ID uživatele MCAUSER”](#) na stránce 364.

### **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 365.

### **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 364.

### **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 blokováno 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 blokováno 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 blokových uživatelů.
  - Pokud se ID uživatele nachází na seznamu blokových uživatelů, kanál bude ukončen.
  - Pokud se ID uživatele nenachází na seznamu blokových uživatelů, kanál bude spuštěn.

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

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

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

<i>Tabulka 7. Pořadí přednosti v podřetězcích</i>		
<b>Pořadí</b>	<b>Podřetězec rozlišujícího názvu</b>	<b>Název</b>
1	SERIALNUMBER=	Sériové číslo certifikátu
2	MAIL=	E-mailová adresa
3	E=	E-mailová adresa (zamítnuto ve prospěch volby MAIL)
4	UID=, USERID=	Identifikátor uživatele
5	CN=	Obecný název
6	T=	Titulek
7	OU=	Organizační jednotka
8	DC=	Komponenta domény
9	O=	Organizace
10	STREET=	Ulice/první řádek adresy

Tabulka 7. Pořadí přednosti v podřetězcích (pokračování)		
Pořadí	Podřetězec rozlišujícího názvu	Název
99,99%	L=	Lokalita
12	ST=, SP=, S=	název státu nebo správního celku
13	PC =	PSC
14	C=	Země
15	UNSTRUCTUREDNAME=	Název hostitele
16	UNSTRUCTUREDADDRESS=	Adresa IP
17	DNQ=	Kvalifikátor rozlišujícího názvu

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

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

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

Pokud jsou dva rozlišující názvy shodné ve všech ohledech kromě svých hodnot DC, platí stejná pravidla porovnání jako u organizačních jednotek, kromě toho, že v hodnotách DC představuje 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

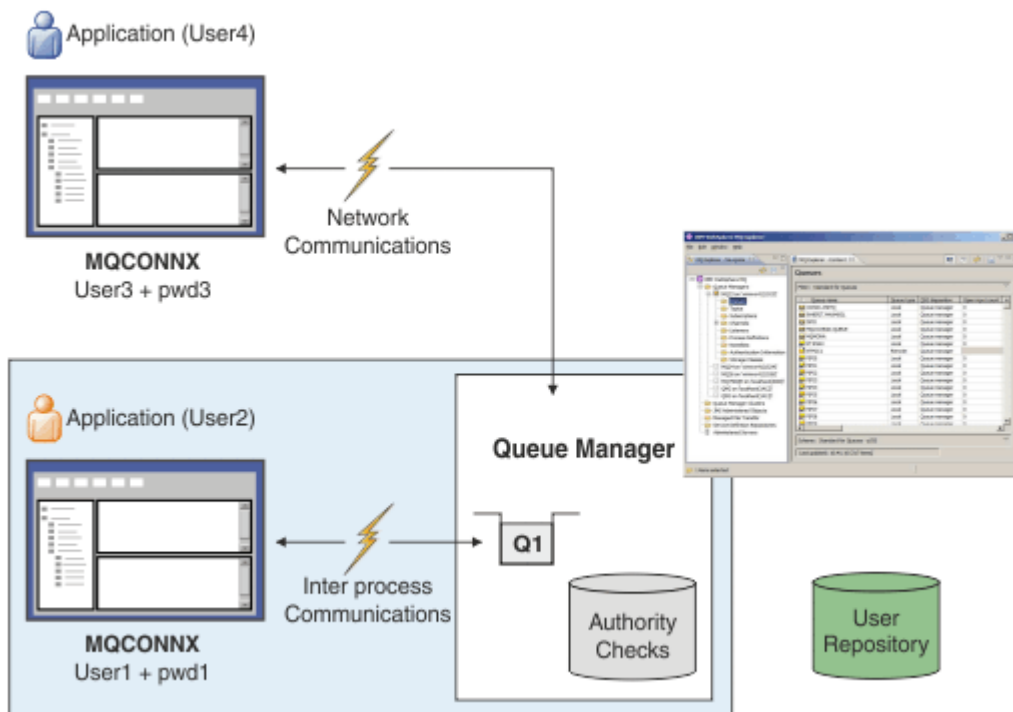
[“Zabezpečení pro vzdálený systém zpráv”](#) na stránce 82

Tento oddíl pojednává o aspektech zabezpečení vzdáleného systému zpráv.

## Ověření připojení

Ověření připojení může být dosaženo různými způsoby:

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



V diagramu se dvě aplikace vytváří připojení ke správci front, jedna aplikace jako klient a jedna s použitím lokálních vazeb. Aplikace mohou používat nejrozličnější rozhraní API pro připojení ke správci front, ale všechny mají schopnost poskytnout ID uživatele a heslo. ID uživatele, pod kterým je aplikace spuštěna, User1 a user3 v diagramu, což je obvyklé ID uživatele operačního systému prezentované produktu IBM MQ, se může lišit od ID uživatele poskytovaného aplikací, User2 a user4.

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

Podrobnosti o úložišti používaném pro kontrolu ID uživatelů a hesel najdete v tématu [Uživatelská úložiště](#).

## Související pojmy

[“Ověřování připojení: Konfigurace”](#) na stránce 56

Správce front může být konfigurován tak, aby používal zadané ID uživatele a heslo a kontroloval, zda má uživatel oprávnění k přístupu k prostředkům.

[“Ověření připojení: Změny aplikace”](#) na stránce 60

[“Ověřování připojení: Uživatelská úložiště”](#) na stránce 61

Pro každého z vašich správců front si můžete vybrat různé typy objektů ověřovacích informací pro ověření ID uživatelů a hesel.

### **Ověřování připojení: Konfigurace**

Správce front může být konfigurován tak, aby používal zadané ID uživatele a heslo a kontroloval, zda má uživatel oprávnění k přístupu k prostředkům.

### **Zapnutí ověření připojení ve správci front**

Na objektu správce front může být atribut **CONNAUTH** nastaven na název objektu ověřovacích informací (AUTHINFO). Tento objekt může být jeden ze dvou typů (atribut AUTHTYPE):

#### **IDPWOS**

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

#### **IDPWLDAP**

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

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

IDPWOS a IDPWLDAP jsou podobné v řadě jejich atributů, které jsou popsány zde. Další atributy jsou považovány za pozdější.

Chcete-li zkontrolovat lokální připojení, použijte atribut AUTHINFO **CHCKLOCL** (zkontrolujte lokální připojení). Chcete-li zkontrolovat připojení klienta, použijte atribut AUTHINFO **CHCKCLNT** (zkontrolujte připojení klienta). Konfigurace musí být aktualizována, než správce front rozpozná změny.

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

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

Oba produkty **CHCKLOCL** a **CHCKCLNT** mají stejnou sadu možných hodnot, které umožňují, aby byla tato omezení rozlišena (variety):

#### **NONE**

Přepne na kontrolu.

#### **Volitelný**

Zajišťuje, že je-li ID uživatele a heslo poskytováno aplikací, jsou to platné dvojice, ale že není povinné je poskytovat. Tato volba může být užitečná během migrace, například.


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

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

#### **POVINNÉ**

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

#### **REQADM**

Oprávnění uživatelé musí zadat platné ID uživatele a heslo, ale s neprivilegovanými uživateli se zachází stejně jako s nastavením VOLITELNÉ . Viz také následující poznámka.  (Toto nastavení není povoleno na systémech z/OS .)

#### **Poznámka:**

Nastavení **CHCKLOCL** na **REQUIRED** nebo **REQDADM** znamená, že nemůžete lokálně spravovat správce front pomocí příkazu **runmqsc** (chyba AMQ8135: Neautorizovaný), pokud uživatel neuvede parametr -u **UserId** na příkazovém řádku **runmqsc** . Při použití této sady produkt **runmqsc** vyzve uživatele k zadání hesla uživatele na konzole.

Podobně platí, že uživatel, který spouští produkt IBM MQ Explorer na lokálním systému, bude při pokusu o připojení ke správci front při pokusu o připojení k správci front zobrazit chybu AMQ4036 . Chcete-li zadat jméno uživatele a heslo, klepněte pravým tlačítkem myši na objekt lokálního správce front a vyberte volbu **Podrobnosti připojení > Vlastnosti ...** . z nabídky. V sekci **ID uživatele** zadejte jméno uživatele a heslo, které má být použito, a poté klepněte na tlačítko **OK**.

Obdobné pokyny platí pro vzdálená spojení s **CHCKCLNT**.

**CONNAUTH** je prázdný pro migrovaná správce front, ale je nastaven na **SYSTEM.DEFAULT.AUTHINFO.IDPWOS** pro nové správce front. Předchozí definice **AUTHINFO** má ve výchozím nastavení **CHCKCLNT** nastaveno na **REQDADM** .

Proto je třeba zadat správné heslo operačního systému pro všechny existující klienty, kteří používají ID privilegovaného uživatele pro připojení.

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

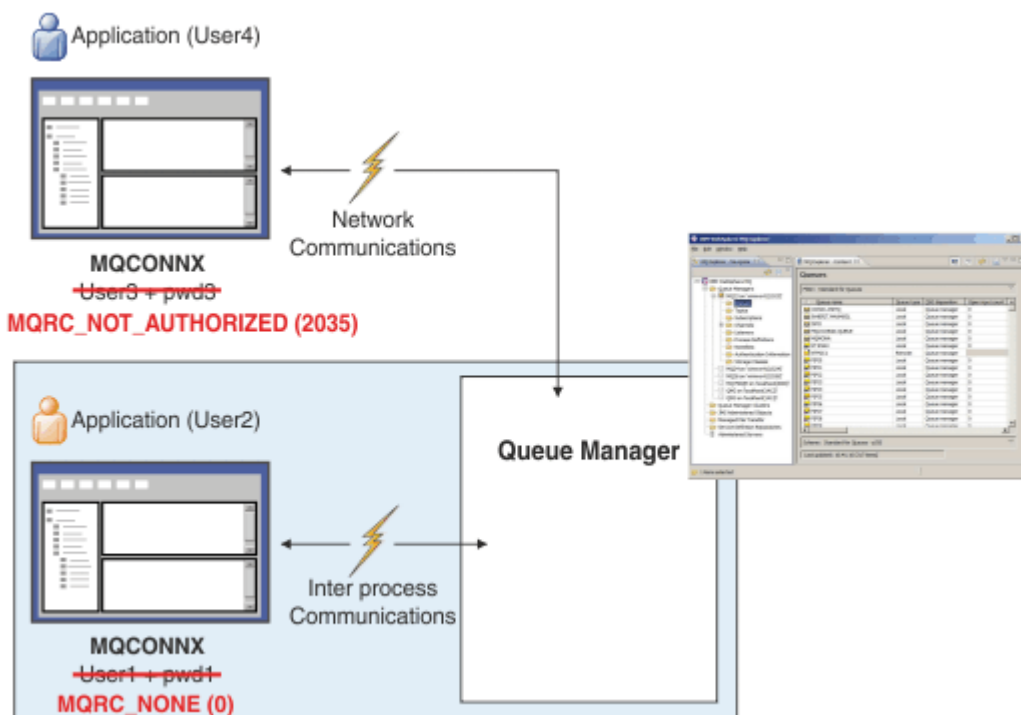
## granularita konfigurace

Kromě produktů **CHCKLOCL** a **CHCKCLNT** , které jsou použity k zapnutí kontroly ID uživatele a hesla, dochází k vylepšení pravidel produktu **CHLAUTH** , takže lze pomocí produktu **CHCKCLNT** provádět specifičtější konfiguraci.

Můžete například nastavit celkovou hodnotu parametru **CHCKCLNT** na hodnotu **VOLITELNÝ** a poté ji upgradovat tak, aby byla pro některé kanály přísnější, nastavením **CHCKCLNT** na hodnotu **REQUIRED** nebo **REQDADM** v pravidle **CHLAUTH** . Standardně se pravidla **CHLAUTH** spustí s produktem **CHCKCLNT (ASQMGR)** , takže tato granularita nebude muset být použita. Příklad:

```
DEFINE AUTHINFO(USE.PW) AUTHTYPE(XXXXXX) +
CHCKCLNT(OPTIONAL)
SET CHLAUTH('*') TYPE(ADDRESSMAP) +
ADDRESS('*') USERSRC(CHANNEL) +
CHCKCLNT(REQUIRED)
SET CHLAUTH('*') TYPE(SSLPEERMAP) +
SSLPEER('CN=*') USERSRC(CHANNEL)
```

## Oznámení o chybě



Chyba se zaznamená, pokud aplikace nedodá uživatelské jméno a heslo, když je požadováno, nebo dodává nesprávnou kombinaci, i když je volitelná.

**Poznámka:** Je-li kontrola hesla vypnuta, pomocí volby NONE v systému **CHKLOCL** nebo **CHKCLNT**, nejsou zjištěna neplatná hesla.

Nezdařené ověření se drží na dobu v sekundách určenou atributem **FAILDLAY**, než se vrátí chyba do aplikace. To poskytuje určitou ochranu z aplikace, která se opakovaně pokouší o připojení.

Chyba se zaznamenává v mnoha ohledech:

### Aplikace

Aplikace je vrácena standardní chyba zabezpečení produktu IBM MQ, RC2035  
-MQRC\_NOT\_AUTHORIZED.

### Administrátor

Administrátor produktu IBM MQ vidí událost nahlášenou v protokolu chyb, a proto může vidět, že aplikace byla odmítnuta, protože ID uživatele a heslo selhalo při kontrole, spíše než například, že například neexistovalo žádné oprávnění k připojení.

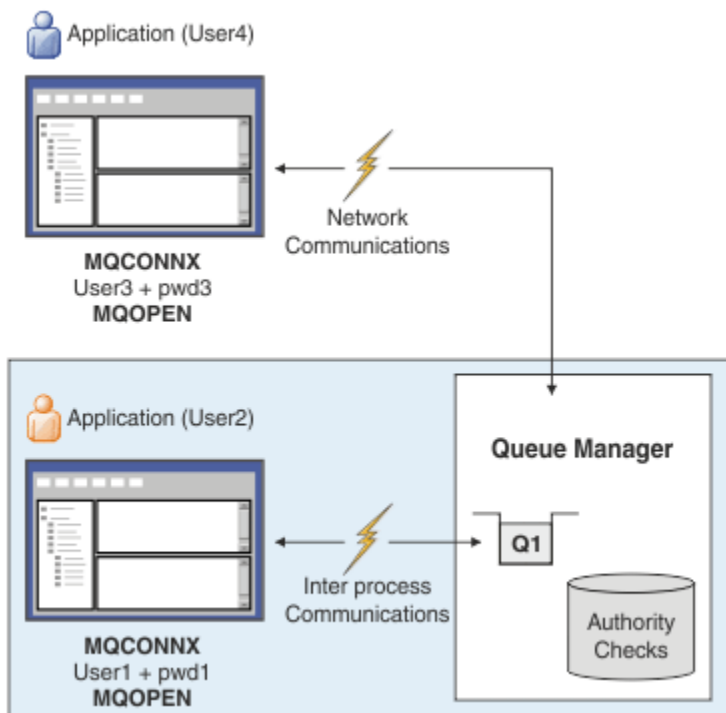
### Monitorovací nástroj

Monitorovací nástroj může být také upozorněn na selhání, pokud zapnete události oprávnění odesláním zprávy o události do SYSTEM.ADMIN.QMGR.EVENT :

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

Tato událost "Bez autorizace" je událost připojení typu 1 a poskytuje stejná pole jako ostatní události typu 1, s dalším polem, ID uživatele MQCSP, které bylo poskytnuto. Heslo není uvedeno ve zprávě o události. To znamená, že ve zprávě události jsou dvě ID uživatelů: ID, pod kterým aplikace běží, a ID, které aplikace prezentovala pro kontrolu ID uživatele a hesla.

## Relace k autorizaci



Správce front můžete nakonfigurovat tak, aby určité ID uživatele a hesla zajišťoval určité aplikace, protože ID uživatele, pod kterým je aplikace spuštěna, nemusí být stejné jako ID uživatele, které aplikace předložila spolu s heslem, když aplikace otevře frontu pro výstup, například:

```
ALTER QMGR CONNAUTH(USE.PWD)
DEFINE AUTHINFO(USE.PWD) +
AUTHTYPE(XXXXXX) +
CHKLOCL(OPTIONAL) +
CHKCLNT(REQUIRED) +
ADOPTCTX(YES)
```

Způsob zpracování uživatelských ID a hesel je řízen atributem **ADOPTCTX** v objektu ověřovacích informací.

### ADOPTCX (ANO)

Všechny kontroly autorizace pro aplikaci se provedou se stejným ID uživatele, které jste ověřeni heslem, výběrem pro převzetí kontextu jako kontextu aplikace pro zbytek životnosti připojení.



**Upozornění:** Když používáte ADOPTCTX (YES) a ID uživatelů OS, musíte se ujistit, že adoptované ID uživatele nepřekročí maximální délku ID uživatelů. Další informace viz [“ID uživatelů”](#) na stránce 70.

### ADOPTCX (NE)

Aplikace poskytuje ID uživatele a heslo pro účely ověření v době připojení, ale pak pokračuje pomocí ID uživatele, pod kterým je aplikace spuštěna, v rámci budoucích kontrol autorizace. Tato volba může být užitečná při migraci nebo v případě, že plánujete použít jiné mechanismy, jako jsou například záznamy ověření kanálu, k přiřazení identifikátoru uživatele agenta kanálu zpráv (MCAUSER).



#### Upozornění:

Použijete-li parametr **ADOPTCTX(YES)** na objektu ověřovacích informací, nelze přijmout další kontext zabezpečení, pokud nenastavíte parametr **ChlauthEarlyAdopt** v sekci kanálů souboru `qm.ini`.

Například výchozí objekt ověřovacích informací je nastaven na **ADOPTCTX(YES)** a uživatel fred je přihlášen. Jsou nakonfigurovány následující dvě pravidla CHLAUTH:

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

Je zadán následující příkaz se záměrem provést ověření příkazu jako schválený kontext zabezpečení uživatele bob:

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

Ve skutečnosti správce front používá kontext zabezpečení produktu fred, nikoli produktu bob, a připojení se nezdaří.

Další informace o příkazu **ChlauthEarlyAdopt** naleznete v tématu [Atributy v sekci kanálů](#).

### Související pojmy

[“Ověření připojení”](#) na stránce 55

[“Ověření připojení: Změny aplikace”](#) na stránce 60

[“Ověřování připojení: Uživatelská úložiště”](#) na stránce 61

Pro každého z vašich správců front si můžete vybrat různé typy objektů ověřovacích informací pro ověření ID uživatelů a hesel.

### **Ověření připojení: Změny aplikace**

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

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

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

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

### **Poznámka:**

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

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

### Související pojmy

[“Ověření připojení”](#) na stránce 55

[“Ověřování připojení: Konfigurace”](#) na stránce 56

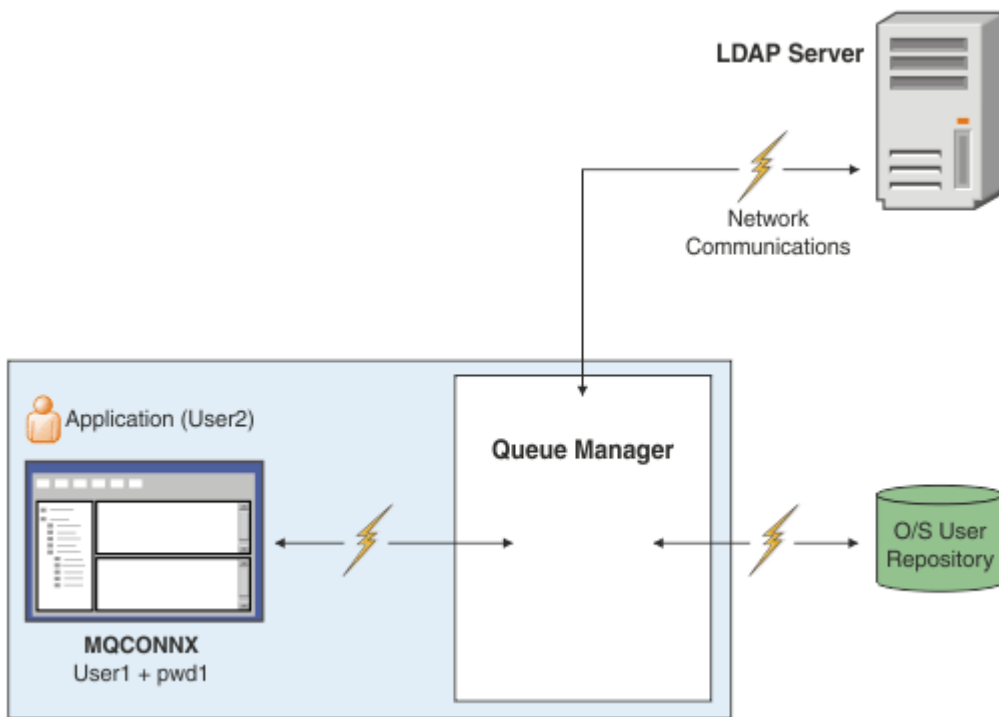
Správce front může být nakonfigurován tak, aby používal zadané ID uživatele a heslo a kontroloval, zda má uživatel oprávnění k přístupu k prostředkům.

[“Ověřování připojení: Uživatelská úložiště”](#) na stránce 61

Pro každého z vašich správců front si můžete vybrat různé typy objektů ověřovacích informací pro ověření ID uživatelů a hesel.

### **Ověřování připojení: Uživatelská úložiště**

Pro každého z vašich správců front si můžete vybrat různé typy objektů ověřovacích informací pro ověření ID uživatelů a hesel.



Obrázek 7. Typy objektů ověřovacích informací

```
DEFINE AUTHINFO(USE.OS) AUTHTYPE(IDPWOS)
DEFINE AUTHINFO(USE.LDAP) +
AUTHTYPE(IDPWLDAP) +
CONNNAME('ldap1(389),ldap2(389)') +
LDAPUSER('CN=QMGR1') +
LDAPPWD('passwd1d') SECCOMM(YES)
```

Existují dva typy objektů ověřovacích informací, jak jsou reprezentovány v diagramu:

- IDPWOS se používá k označení toho, že správce front používá lokální operační systém k ověření jména uživatele a hesla. Rozhodnete-li se používat lokální operační systém, je třeba nastavit pouze běžné atributy, jak je popsáno v předchozích tématech.
- IDPWLDAP se používá k označení toho, že správce front používá server LDAP k ověření ID uživatele a hesla. Rozhodnete-li se používat server LDAP, jsou k dispozici další informace.

Pro každého správce front může být vybrán pouze jeden typ objektu ověřovacích informací, tím, že pojmenováváte odpovídající objekt v atributu **CONNAUTH** správce front.

### **Použití serveru LDAP pro ověření.**

Nastavte pole **CONNNAME** na adresu serveru LDAP pro správce front. Pro server LDAP můžete zadat další adresy v seznamu odděleném čárkami, který může pomoci s redundancí, pokud server LDAP tuto poskytovanou službu neposkytuje sám.

V polích **LDAPUSER** a **LDAPPWD** nastavte požadované ID a heslo serveru LDAP tak, aby správce front mohl přistupovat k serveru LDAP a vyhledávat informace o uživatelských záznamech.



## Zabezpečené připojení k serveru LDAP

Na rozdíl od kanálů není k dispozici žádný parametr **SSLCIPH** pro zapnutí použití protokolu SSL/TLS pro komunikaci se serverem LDAP. V tomto případě se IBM MQ chová jako klient na serveru LDAP, takže velká část konfigurace se provádí na serveru LDAP. Některé existující parametry v produktu IBM MQ se používají ke konfiguraci toho, jak toto připojení funguje.

Nastavte pole **SECCOMM**, které řídí, zda konektivita k serveru LDAP používá SSL/TLS.

Kromě tohoto atributu omezují atributy správce front **SSLFIPS** a **SUITEB** sadu specifikací šifer, které jsou vybrány. Certifikát, který se používá k identifikaci správce front na serveru LDAP, je certifikát správce front, buď `ibmwebspheremq <qmgr-name>`, nebo hodnota atributu **CERTLABL**. Podrobnosti najdete v tématu [Digitální certifikáty certifikátu](#).

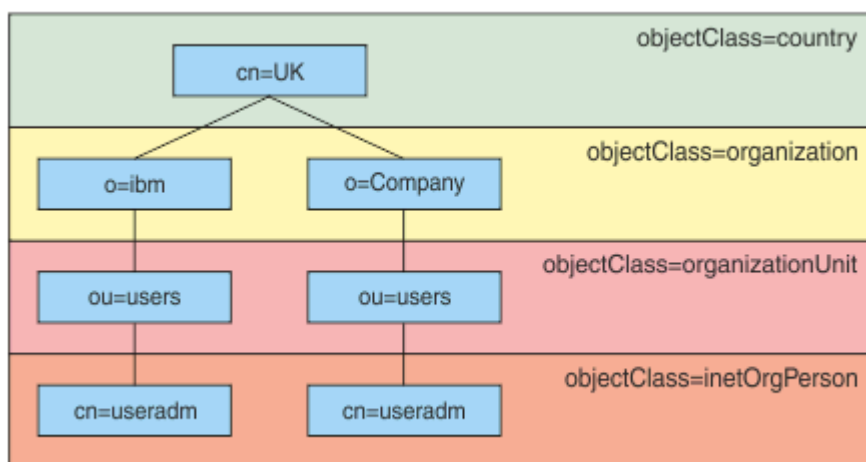
## Úložiště uživatelů LDAP

Při použití úložiště uživatelů LDAP je třeba na správci front provést další konfiguraci, než stačí říct správci front, kde má najít server LDAP.

ID uživatelů definovaná na serveru LDAP mají hierarchickou strukturu, která je jedinečně identifikuje. Aplikace se proto může připojit ke správci front a prezentovat své ID uživatele jako úplné hierarchické ID uživatele.

Chcete-li však zjednodušit informace, které má aplikace poskytnout, je možné správce front nakonfigurovat tak, aby předpokládal, že první část hierarchie je společná pro všechna ID, a automaticky ji přidat před zkráceným ID, které poskytuje aplikace. Správce front poté může předložit úplné ID na server LDAP.

Nastavte **BASEDNU** na počáteční bod, který vyhledávání LDAP vyhledá ID v hierarchii LDAP. Když nastavíte **BASEDNU**, musíte zajistit, aby byl vrácen pouze jeden výsledek při hledání ID v hierarchii LDAP.



Obrázek 8. Příklad hierarchie LDAP

Například v souboru [Obrázek 8](#) na stránce 62 **BASEDNU** může být nastavena hodnota "ou=users, o=ibm, c = UK" nebo ", o=ibm, c = UK". Protože však rozlišující název, který obsahuje "cn = useradm", existuje ve větvi "o = ibm" a větev "o=Company", nelze parametr **BASEDNU** nastavit na hodnotu "c = UK". Z důvodů výkonu a zabezpečení použijte nejvyšší bod v hierarchii LDAP, ze kterého můžete odkazovat na všechna ID uživatelů, které potřebujete. V tomto příkladě to je "ou=users, o=ibm, c = UK".

Vaše aplikace může odeslat správci front ID uživatele, aniž by poskytoval název atributu LDAP, například **CN=**. Nastavíte-li parametr **USRFIELD** na název atributu LDAP, bude tato hodnota přidána jako předpona k ID uživatele, které pochází z aplikace. To může být užitečná migrační podpora při přechodu z ID uživatelů operačního systému na ID uživatelů LDAP, protože aplikace pak může v obou případech předložit stejný řetězec a vy se můžete vyhnout změnám v aplikaci.

Úplné ID uživatele představené na serveru LDAP proto vypadá takto:

```
<USRFIELD> = <ID_from_application> <BASEDNU>
```

### Související pojmy

“Ověření připojení” na stránce 55

“Ověřování připojení: Konfigurace” na stránce 56

Správce front může být konfigurován tak, aby používal zadané ID uživatele a heslo a kontroloval, zda má uživatel oprávnění k přístupu k prostředkům.

“Ověření připojení: Změny aplikace” na stránce 60

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

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

## Přehled

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

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

## Umístění

**mqccred** je nainstalován:

### Windows platformy

V adresáři `<installation directory>\Tools\c\Samples\mqccred\`

### SYSTÉM UNIX

V adresáři `<installation_directory>/samp/mqccred`

**Notes:** Výjezd:

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

Například na 64bitovém počítači platformy UNIX zadejte příkaz:

```
cp <installation_directory>/samp/mqccred/lib64/* /var/mqm/exits
```

Další informace viz Příklad testu mqccred krok za krokem.

4. Je schopen běžet na předchozích verzích produktu IBM MQ ; co nejdál Verze 7.0.1.

## Nastavení ID uživatele a hesel

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

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

Popis příkazu a jeho parametrů viz [runmqccred](#).

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

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

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

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

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

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

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

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

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

Pro všechny správce front nebo pro každého jednotlivého správce front můžete zadat ID uživatele a heslo. Toto je příklad souboru `mqccred.ini`:

```
# comments are permitted
AllQueueManagers:
User=abc
OPW=%^&aervrgtsr

QueueManager:
Name=QMA
User=user1
OPW=H&^dbgfH

Force=TRUE

QueueManager:
Name=QMB
User=user2
password=passw0rd
```

### Notes:

1. Jednotlivé definice správců front mají přednost před globálním nastavením.
2. Atributy nerozlišují velikost písmen.

## Omezení

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

Proto je třeba správce front nakonfigurovat tak, aby používal produkt **ADOPTCTX(YES)**, nebo namapovat požadavek na příchozí připojení na příslušné ID uživatele prostřednictvím jednoho z dostupných mechanismů, například “Záznamy ověření kanálu” na stránce 48.

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

## Ladění

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

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

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

### CHYBA

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

### LADĚNÍ

Zobrazí tyto chybové stavy a některé další trasovací příkazy.

### NEKONTROLY

Vynechá omezení pro oprávnění k souboru a dále omezení, že by soubor `.ini` neměl obsahovat žádná nechráněná hesla.

Do pole **SCYDATA** můžete vložit jeden nebo více těchto prvků, oddělených čárkami, v libovolném pořadí. Například `SCYDATA=(NOCHECKS,DEBUG)`.

Všimněte si, že položky jsou citlivé na velikost písmen a musí být zadány velkými písmeny.

## Použití produktu mqccred

Po nastavení vašeho souboru můžete volat uživatelskou proceduru aktualizací své definice kanálu připojení klienta tak, aby obsahovala atribut `SCYEXIT('mqccred(ChlExit)')` :

```
DEFINE CHANNEL(<channelname>) CHLTYPE(cIntconn) +  
CONNAME(<remote machine>) +  
QMNAME(<remote qmgr>) +  
SCYEXIT('mqccred(ChlExit)') +  
REPLACE
```

### Související informace

[SCYDATA](#)

[SCYEXIT](#)

[runmqccred](#)

### Ověření spojení s klientem Java

Ověření připojení je funkcí v produktu IBM MQ, které umožňuje konfiguraci správce front za účelem ověření aplikací pomocí poskytnutého ID uživatele a hesla. Je-li aplikace aplikací produktu Java s použitím vazeb klienta, existují dva režimy, ve kterých lze tuto aplikaci spustit.

### Režim kompatibility

Ve verzích starších než IBM MQ 8.0 mohl klient produktu Java odeslat ID uživatele a heslo přes kanál připojení klienta k kanálu připojení serveru a nechat je v polích **RemoteUserIdentifier**

a **RemotePassword** struktury MQCD k dispozici pro ukončení zabezpečení. V režimu kompatibility je toto chování zachováno.

Tento režim můžete použít v kombinaci s ověřením připojení a migrovat z jakýchkoli uživatelských procedur zabezpečení, které byly dříve použity pro provedení stejné úlohy.

Musíte použít parametr ADOPTCTX (YES) nebo použít jinou metodu, například pravidlo CHLAUTH založené na certifikátu SSL/TLS, nastavit spuštění MCAUSER při použití režimu kompatibility, jako v tomto režimu, ID uživatele na straně klienta není odesláno správci front.

Režim kompatibility je výchozí nastavení.

## Režim ověření MQCSP

V tomto režimu se odešle ID uživatele na straně klienta a ID uživatele a heslo pro ověření, takže můžete použít ADOPTCTX (NO). ID uživatele a heslo jsou k dispozici pro uživatelskou proceduru zabezpečení připojení k serveru ve struktuře MQCSP obsažené ve struktuře MQCXP.

Tento režim operace lze povolit na bázi připojení po připojení nebo globálně:

- V produktu IBM MQ classes for Javanastavte vlastnost *MQConstants.USE MQCSP AUTHENTICATION PROPERTY* na hodnotu **true** v hašovací tabulce vlastností předané konstruktoru produktu **com.ibm.mq.MQQueueManager**.
- V produktu IBM MQ classes for JMSnastavte vlastnost *JmsConstants.USER AUTHENTICATION MQCSP* na hodnotu **true** u příslušné továrny připojení před vytvořením připojení.
- Globálně nastavte systémovou vlastnost *com.ibm.mq.cfg.jmqi.useMQCSPauthentication* na hodnotu indikující hodnotu true, například přidáním `-Dcom.ibm.mq.cfg.jmqi.useMQCSPauthentication=Y` do příkazového řádku.

## Povolení režimu ověřování MQCSP v Průzkumníku IBM MQ

MQ Explorer je aplikace Java, takže se tyto dva režimy vztahují i na tento režim.

Stejně jako u jiných aplikací produktu Java je režim kompatibility výchozí.

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

Ve výchozím nastavení je toto zaškrťovací políčko povoleno. Chcete-li použít ověření MQCSP, odeberte zaškrtnutí z tohoto rámečku.

### Související pojmy

[“Ověření připojení”](#) na stránce 55

[“Ověření připojení: Změny aplikace”](#) na stránce 60

[“Ověřování připojení: Uživatelská úložiště”](#) na stránce 61

Pro každého z vašich správců front si můžete vybrat různé typy objektů ověřovacích informací pro ověření ID uživatelů a hesel.

## Zabezpečení zpráv v produktu IBM MQ

Zabezpečení zpráv v infrastruktuře produktu IBM MQ je poskytováno IBM MQ Advanced Message Security.

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

### Související pojmy

[“IBM MQ Advanced Message Security”](#) na stránce 438



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

## Plánování bezpečnostních požadavků

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





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

Produkt IBM MQ poskytuje rozsah služeb zabezpečení na úrovni odkazu, včetně podpory zabezpečení SSL (Secure Sockets Layer) a TLS (Transport Layer Security).



Při implementaci produktu WebSphere je třeba vzít v úvahu určité aspekty zabezpečení. Pokud v systémech  IBM i, UNIX, Linux a Windows ignorujete tyto aspekty a nedělat nic, nemůžete použít produkt IBM MQ.  V systému z/OS je výsledkem ignorování těchto aspektů to, že vaše prostředky IBM MQ jsou nechráněné. To znamená, že všichni uživatelé mohou přistupovat a měnit všechny prostředky IBM MQ .

### Oprávnění ke správě produktu IBM MQ

Administrátoři produktu IBM MQ potřebují oprávnění k:

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

Další informace naleznete v následujících tématech:

- [“Oprávnění k administraci produktu IBM MQ v systémech SYSTÉM UNIX, Linuxu a Okna” na stránce 377](#)
-  [“Oprávnění ke správě produktu IBM MQ v systému IBM i” na stránce 72](#)
-  [“Oprávnění ke správě produktu IBM MQ v systému z/OS” na stránce 73](#)

### Oprávnění pro práci s objekty IBM MQ

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

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

Aplikace mohou také používat příkazy PCF (Programmable Command Format) pro přístup k těmto objektům IBM MQ a také k přístupu k kanálům a objektům ověřovacích informací. Tyto objekty mohou být chráněny produktem IBM MQ tak, aby ID uživatelů přidružená k aplikacím potřebují oprávnění pro přístup k nim.

Další informace viz [“Autorizace pro aplikace, které mají být použity IBM MQ” na stránce 74.](#)

## Zabezpečení kanálu

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

Další informace viz [“Ověřování kanálu”](#) na stránce 95.

## Další pokyny

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

- [“Zabezpečení klastrů správců front”](#) na stránce 107
- [“Zabezpečení pro publikování/odběr produktu IBM MQ”](#) na stránce 107
- [“Zabezpečení pro IBM MQ internet pass-thru”](#) na stránce 109

## Plánování identifikace a ověření

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

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

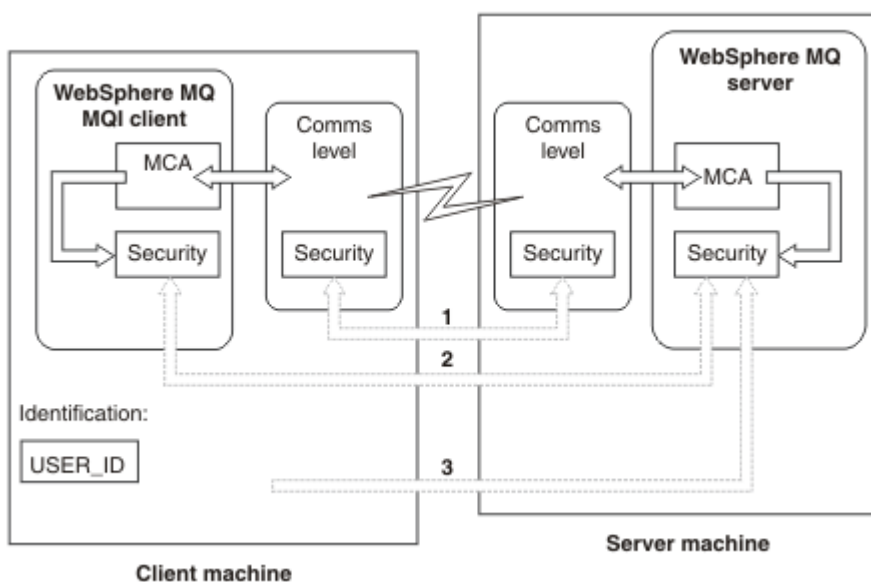
- [“Mapování vzdáleného správce front na ID uživatele MCAUSER”](#) na stránce 364
- [“Mapování uživatelem deklarovaného ID uživatele na ID uživatele MCAUSER”](#) na stránce 364
- [“Mapování rozlišovacího jména SSL nebo TLS na ID uživatele MCAUSER”](#) na stránce 365
- [“Mapování adresy IP na ID uživatele MCAUSER”](#) na stránce 367

## Plánování ověření pro klientskou aplikaci

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

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





Obrázek 9. Zabezpečení v připojení klient/server

#### 1. Úroveň komunikace

Viz šipka 1. Chcete-li implementovat zabezpečení na úrovni komunikace, použijte SSL nebo TLS. Další informace naleznete v tématu [“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 nasadit ID uživatele namapovat na platné ID uživatele. Úplný popis je uveden v tématu [“Záznamy ověření kanálu”](#) na stránce 48.

#### 3. Ověření připojení

Viz šipka 3. Klient odešle ID a heslo. Další informace viz [“Ověřování připojení: Konfigurace”](#) na stránce 56.

#### 4. Uživatelské procedury zabezpečení kanálu

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

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

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

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 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 320. Další informace

o definování záznamů ověření kanálu viz [“Mapování uživatelem deklarovaného ID uživatele na ID uživatele MCAUSER”](#) na stránce 364.




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

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

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

## ID uživatelů

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

-  V systémech z/OS a SYSTÉM UNIX a Linux je maximální délka ID uživatele 12 znaků.
-  V systému IBM i je maximální délka ID uživatele 10 znaků.
-  Pokud je v systému Windows server IBM MQ MQI client server IBM MQ na serveru Windowsa server má přístup k doméně, na které je ID uživatele klienta definováno, maximální délka ID uživatele je 20 znaků. Pokud však server IBM MQ není server Windows, je ID uživatele oříznuto na 12 znaků.
- Pokud k předávání pověření používáte strukturu MQCSP, maximální délka ID uživatele je 1024 znaků. ID uživatele struktury MQCSP nelze použít k obejití maximální délky ID uživatele používaného produktem IBM MQ pro autorizaci. Další informace o struktuře MQCSP viz [“Identifikace a ověřování uživatelů pomocí struktury MQCSP”](#) na stránce 319.

Na systémech SYSTÉM UNIX a Linux se standardně používají ID uživatelů k ověření a skupiny se používají pro autorizaci. Tyto systémy však můžete nakonfigurovat tak, aby bylo možné autorizovat k ID uživatelů. Další informace naleznete v tématu [Oprávnění založená na uživateli OAM v systémech SYSTÉM UNIX a Linux](#). Systémy Windows mohou používat jak ID uživatele pro ověření, tak i autorizaci a skupiny pro autorizaci.

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

## Omezená ID uživatelů

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

## ID uživatelů při připojování k serveru IBM MQ for Windows

### Windows

Server IBM MQ for Windows nepodporuje připojení 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.

## Plánování autorizace

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

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

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




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

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

### Oprávnění ke správě produktu IBM MQ

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

Administrátoři produktu IBM MQ potřebují oprávnění k:

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

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

### Oprávnění k administraci produktu IBM MQ v systémech UNIX a Windows

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

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

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

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


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

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

Program IBM MQ Explorer vydává příkazy PCF pro provádění administrativních úloh. Administrátoři nepotřebují další oprávnění k používání Průzkumníka IBM MQ ke správě správce front v lokálním systému.

Pokud se Průzkumník IBM 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 prováděných při zpracování příkazů PCF a MQSC naleznete v následujících tématech:

- Pro příkazy, které pracují se správci front, frontami, kanály, procesy, seznamy názvů a ověřovacími informacemi, viz [“Autorizace pro aplikace, které mají být použity IBM MQ”](#) na stránce 74.
- Pro příkazy, které pracují s kanály, inicializátory kanálu, listenery a klastry, naleznete informace v tématu [Zabezpečení kanálů](#).
-  Pro příkazy MQSC, které jsou zpracovány příkazovým serverem v systému IBM MQ for z/OS, viz téma [“Zabezpečení příkazů a zabezpečení prostředků příkazů”](#) na stránce 73.

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

## **Oprávnění ke správě produktu IBM MQ v systému IBM i**

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

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

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

### **Skupina 1**

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

### **Skupina 2**

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

- Uživatel vyžaduje oprávnění IBM i k použití příkazu. Toto oprávnění je uděleno pomocí příkazu GRTOBJAUT.
- Uživatel vyžaduje oprávnění IBM MQ pro přístup k libovolnému objektu IBM MQ přidruženému k příkazu. Toto oprávnění je uděleno pomocí příkazu GRTRMQMAUT.

Zde jsou příklady příkazů v této skupině:

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

Další informace o této skupině příkazů najdete v tématu [“Autorizace pro aplikace, které mají být použity IBM MQ”](#) na stránce 74.

Úplný seznam příkazů skupiny 1 a skupiny 2 najdete v tématu [“Přístupová oprávnění pro objekty IBM MQ v systému IBM i”](#) na stránce 144 .

Další informace o oprávnění, které potřebujete ke správě produktu IBM MQ v systému IBM i, najdete v tématu [Administrace produktu IBM i](#) .

## Oprávnění ke správě produktu IBM MQ v systému z/OS

Tato kolekce témat popisuje různé aspekty oprávnění, které potřebujete ke správě produktu IBM MQ for z/OS.

### Kontroly oprávnění v systému z/OS

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

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

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

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

#### **zabezpečení na úrovni skupiny sdílení front**

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

#### **zabezpečení na úrovni správce front**

Kontroly oprávnění používají profily produktu RACF specifické pro správce front.

Můžete použít kombinaci skupiny sdílení front a zabezpečení na úrovni správce front. Můžete například zajistit, aby profily specifické pro správce front potlačovali profily skupin sdílení front, do kterých patří.

Zabezpečení subsystému, zabezpečení na úrovni skupiny sdílení front a zabezpečení na úrovni správce front jsou zapnuty nebo vypnuty definováním *profilů přepínače*. Profil přepínače je normální profil RACF , který má speciální význam pro IBM MQ.

### *Zabezpečení příkazů a zabezpečení prostředků příkazů*

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

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

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

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

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

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

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

jsou provedeny následující kontroly oprávnění:

- Příkaz Security Security kontroluje, že administrátor je oprávněn vydávat příkaz DEFINE QLOCAL.

- Kontrola zabezpečení prostředků příkazů kontroluje, zda je administrátor oprávněn provádět operaci s lokální frontou s názvem MOON.EUROPA.

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

#### *Příkazy MQSC a vstupní fronta systémových příkazů*

Toto téma vám pomůže pochopit, jak příkazový server zpracovává příkazy MQSC, které jsou směřovány do vstupní fronty systémových příkazů.

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

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

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

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

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

#### *Přístup k datovým sadám správce front*

Administrátoři produktu IBM MQ potřebují oprávnění pro přístup k datovým sadám správce front. Toto téma vám pomůže porozumět, které datové sady potřebují ochranu produktu RACF.

Tyto datové sady zahrnují:

- Datové sady odkazované podle CSQINP1, CSQINP2, CSQINPT a CSQXLIB v proceduře spuštěné úlohy správce front
- Sady stránek správce front, datové sady aktivního žurnálu, datové sady protokolu archivu a zaváděcí datové sady (BSDs).
- Datové sady odkazované podle CSQXLIB a CSQINPX v proceduře spuštěné úlohy inicializátoru kanálu

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

## **Autorizace pro aplikace, které mají být použity IBM MQ**

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

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

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


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

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

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

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

MCAs také vydává volání MQI a ID uživatelů přidružená k MCAs potřebují oprávnění pro přístup k těmto objektům IBM MQ . Další informace o těchto ID uživatelů a oprávněních, která vyžadují, najdete v tématu [“Ověřování kanálu”](#) na stránce 95.

V systému z/OS mohou aplikace také používat příkazy MQSC pro přístup k těmto objektům produktu IBM MQ , ale zabezpečení příkazů a zabezpečení prostředků příkazů zajišťují oprávnění ke kontrole oprávnění za těchto okolností.  Další informace viz [“Zabezpečení příkazů a zabezpečení prostředků příkazů”](#) na stránce 73 a [“Příkazy MQSC a vstupní fronta systémových příkazů”](#) na stránce 74.

V systému IBM může uživatel, který vydává příkaz CL ve skupině 2, vyžadovat oprávnění pro přístup k objektu IBM MQ přidruženému k příkazu. Další informace viz [“Při provádění kontrol oprávnění”](#) na stránce 75.

### ***Při provádění kontrol oprávnění***

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

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

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

Správce front požádá operační systém o ID uživatele přidruženého k aplikaci. Správce front poté ověří, zda je ID uživatele oprávněno k jeho připojení, a zachová ID uživatele pro budoucí kontroly.

Uživatelé se nemusí přihlašovat k produktu IBM MQ. Produkt IBM MQ předpokládá, že uživatelé jsou přihlášení k základnímu operačnímu systému a že jsou ověřeni pomocí tohoto systému.

#### **Když aplikace otevře objekt IBM MQ pomocí volání MQOPEN nebo MQPUT1**

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

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

Když aplikace otevře frontu, provede se kontrola oprávnění k objektu uvedenému v poli `ObjectName` v deskriptoru objektu. Pole `ObjectName` se používá na voláních `MQOPEN` nebo `MQPUT1` . Je-li objekt alias fronta nebo definice vzdálené fronty, kontroly oprávnění se provádějí proti objektu samotnému.



Nejsou prováděny ve frontě, na kterou je rozlišována fronta aliasů nebo definice vzdálené fronty. To znamená, že uživatel nepotřebuje oprávnění pro přístup k němu. Omezte oprávnění k vytváření front pro privilegované uživatele. Pokud tomu tak není, uživatelé mohou obejít normální řízení přístupu pouhým vytvořením aliasu.

Aplikace může explicitně odkazovat na vzdálenou frontu. Nastaví pole `ObjectName` a `ObjectQMgrName` v deskriptoru objektu na názvy vzdálené fronty a vzdáleného správce front. Kontroly oprávnění se provádějí proti přenosové frontě se stejným názvem jako vzdáleným správcem front. V systému z/OS je na profilu fronty produktu RACF, který odpovídá názvu vzdáleného správce front, provedena kontrola. Na jiných platformách než z/OS je kontrola provedena proti profilu RQMNAME, který odpovídá názvu vzdáleného správce front, je-li použito 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 přihlášená k odběru, ve stromu témat nebo nad nimi. Kontroly oprávnění mohou zahrnovat kontroly více než jednoho objektu tématu. ID uživatele, které správce front používá pro kontrolu oprávnění, je získáno z operačního systému. ID uživatele se získá, když se aplikace připojí ke správci front.

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

#### **Když aplikace odstraní trvalou dynamickou frontu pomocí volání `MQCLOSE`**

Popisovač objektu zadaný ve volání `MQCLOSE` nemusí být nutně stejný jako popisovač vrácený voláním `MQOPEN`, který vytvořil trvalou dynamickou frontu. Pokud se liší, správce front zkontroluje ID uživatele přidružené k aplikaci, která vydala volání `MQCLOSE`. Kontroluje, zda je ID uživatele autorizováno k odstranění fronty.

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

#### **Když je příkaz `PCF`, který pracuje na objektu `IBM MQ`, zpracován příkazovým serverem**

Toto pravidlo zahrnuje případ, kdy příkaz `PCF` pracuje s objektem ověřovacích informací.

ID uživatele, který se použije pro kontrolu oprávnění, je ten, který se nachází v poli `UserIdentifier` v deskriptoru zpráv příkazu `PCF`. Toto ID uživatele musí mít požadovaná oprávnění ve správci front, ve kterém je příkaz zpracováván. Ekvivalentní příkaz `MQSC` zapouzdřený v rámci příkazu `Escape PCF` je zpracován stejným způsobem. Další informace o poli `UserIdentifier` a o tom, jak je nastaveno, viz [“kontext zprávy” na stránce 77](#).

### **IBM i V systému IBM i, když uživatel vydává příkaz `CL` ve skupině 2, který pracuje na objektu `IBM MQ`**

Toto pravidlo zahrnuje případ, kdy příkaz `CL` ve skupině 2 pracuje na objektu ověřovacích informací.

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

Naproti tomu příkaz **DSPMQMQ**, který zobrazuje frontu MQM, vyžaduje oprávnění k zobrazení atributů fronty určené příkazem.

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

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

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

### **Oprávnění alternativního uživatele**

Když aplikace otevře objekt nebo se přihlásí k odběru tématu, může aplikace dodat ID uživatele v rámci volání MQOPEN, MQPUT1 nebo 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 MQ na systémech IBM i, UNIX, Linux a Windows**

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

### **• Ověřování.**

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

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

- Pokud byla struktura MQCSP dodána připojovanou aplikací, a
- Atribut *AuthenticationType* ve struktuře MQCSP má hodnotu MQCSP\_AUTH\_USER\_ID\_AND\_PWD a
- Hodnota CHCKLOCL nebo CHKCLLNT na konfigurovaném objektu AUTHINFO není 'NONE'


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

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

- Autorizace.

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


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

U systémů  IBM i, UNIX, Linux a Windows poskytuje *autorizační služba* řízení přístupu, když aplikace vydá volání MQI pro přístup k objektu IBM MQ, který je správcem front, frontou, procesem, tématem nebo seznamem názvů. To zahrnuje kontroly pro alternativní oprávnění uživatele a oprávnění k nastavení nebo předání informací o kontextu.

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

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


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

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

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

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

OAM udržuje seznam přístupových práv (ACL) pro každý objekt produktu IBM MQ, ke kterému má oprávnění přístup. V systémech SYSTÉM UNIX a Linux se mohou v seznamu přístupových práv zobrazit pouze ID skupin. To znamená, že všichni členové skupiny mají stejné oprávnění. Na systémech

 IBM i a na Windows se mohou v seznamu ACL objevit jak ID uživatele, tak ID skupin. To znamená, že oprávnění mohou být udělována jednotlivým uživatelům a skupinám.

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

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

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

U systémů UNIX, Linux a Windows, řídicí příkaz **setmqaut** uděluje a odvolává oprávnění a používá se k údržbě seznamů ACL. Například příkaz:

```
setmqaut -m JUPITER -t queue -n MOON.EUROPA -g VOYAGER +browse +get
```

Umožňuje členům skupiny VOYAGER procházet zprávy ve frontě MOON.EUROPA, 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**.

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

**IBM i** Administrátor v systému IBM i používá příkaz CL GRMQMAUT k udělení oprávnění a CL příkaz RVMQMAUT k odvolání oprávnění. Lze také použít generické profily. Například CL příkaz:

```
GRMQMAUT MQMNAME(JUPITER) OBJTYPE(*Q) OBJ('MOON.*') USER(VOYAGER) AUT(*PUT)
```

poskytuje stejnou funkci jako předchozí příklad příkazu **setmqaut**; umožňuje členům skupiny VOYAGER vkládat zprávy do jakékoli fronty se jménem, které začíná znaky MOON.

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

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

*Použití příkazu PCF pro přístup k příkazům OAM*

Na systémech **IBM i** IBM i, UNIX, Linux a Windows můžete použít příkazy PCF pro přístup k příkazům administrace OAM.

Příkazy PCF a jejich ekvivalentní příkazy OAM jsou následující:

<i>Tabulka 8. Příkazy PCF a jejich ekvivalentní příkazy OAM</i>	
<b>příkaz PCF</b>	<b>příkaz OAM</b>
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](#).

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

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

Sedm kategorií kontrol oprávnění souvisejících s voláními do rozhraní MQI:

### **Zabezpečení připojení**

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

### **Zabezpečení fronty**

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

### **Zabezpečení procesu**

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

### **Zabezpečení seznamu názvů**

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

### **alternativní zabezpečení uživatele**

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

### **zabezpečení kontextu**

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

### **Zabezpečení tématu**

Kontroly oprávnění, které jsou provedeny při otevření tématu aplikace.

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

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

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

Všechny kategorie, kromě zabezpečení připojení, jsou souhrnně označovány jako *zabezpečení na úrovni rozhraní API*.

Je-li v důsledku volání MQI z aplikace pomocí dávkového připojení provedena kontrola zabezpečení pomocí rozhraní API, je zkontrolováno pouze jedno ID uživatele, pokud je kontrola zabezpečení prostředku API provedena. Je-li kontrola provedena jako výsledek volání MQI z aplikace CICS nebo IMS, nebo z inicializátoru kanálu, jsou zkontrolována dvě ID uživatelů.

Definováním *profilu RESLEVEL* však můžete řídit, zda jsou zaškrtnuta nula, jedna nebo dvě ID uživatelů. Počet ID uživatelů, které jsou zkontrolovány, je určen ID uživatele přidruženého k typu připojení, když se aplikace připojí ke správci front a úroveň přístupu, kterou má ID uživatele k profilu *RESLEVEL*. ID uživatele přidružené ke každému typu připojení je:

- ID uživatele připojované úlohy pro dávkové připojení
- ID uživatele adresního prostoru CICS pro připojení CICS
- ID uživatele adresního prostoru IMS pro připojení IMS
- ID uživatele adresního prostoru iniciátoru kanálu pro připojení inicializátoru kanálu

Další informace o oprávnění pro práci s objekty produktu IBM MQ v systému z/OS naleznete v tématu [“Oprávnění ke správě produktu IBM MQ v systému z/OS” na stránce 73](#).

## Zabezpečení pro vzdálený systém zpráv

Tento oddíl pojednává o aspektech zabezpečení vzdáleného systému zpráv.

Musíte uživatelům poskytnout oprávnění k používání zařízení produktu IBM MQ . To je organizováno v závislosti na akcích, které mají být provedeny s ohledem na objekty a definice. Příklad:

- Správci front mohou být spuštěni 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 IBM MQ for IBM i

Tento oddíl pojednává o aspektech zabezpečení vzdáleného systému zpráv.

Musíte poskytnout uživatelům s oprávněním, aby mohli využívat zařízení produktu IBM MQ for IBM i . Toto oprávnění je organizováno v závislosti na akcích, které mají být provedeny s ohledem na objekty a definice. Příklad:

- Správci front mohou být spuštěni a zastaveni autorizovanými uživateli.
- Aplikace se musí připojit ke správci front a mají oprávnění pro použití front.
- Kanály zpráv musí být vytvořeny a řízeny oprávněnými uživateli.

Agent kanálu zpráv na vzdáleném serveru musí zkontrolovat, zda je doručovaná zpráva odvozena od uživatele s oprávněním, aby zadal zprávu na tomto vzdáleném serveru. Kromě toho je možné, že jako MCAs může být spuštěno vzdáleně, může být nezbytné ověřit, zda se vzdálené procesy pokoušejí spustit vaše MCA, k tomu mají oprávnění. Existují čtyři možné způsoby, jak se s tím vypořádat:

- Vyhláška v definici kanálu, že zprávy musí obsahovat přijatelný *kontext* oprávnění, jinak budou zahozeny.
- Chcete-li odmítnout nechtěné pokusy o připojení nebo nastavit hodnotu MCAUSER na základě jedné z následujících možností: vzdálenou adresu IP, jméno vzdáleného uživatele, rozlišující název SSL nebo TLS nebo název vzdáleného správce front, implementujte záznamy ověření kanálu pro zamítnutí nechtěných pokusů o připojení nebo nastavte hodnotu MCAUSER.
- Implementujte kontrolu zabezpečení ukončení uživatele, abyste se ujistili, že je odpovídající kanál zpráv autorizován. Zabezpečení instalace hostujícího odpovídající kanál zajišťuje, aby všichni uživatelé byli řádně autorizováni, takže nemusíte kontrolovat jednotlivé zprávy.
- Implementujte zpracování zpráv *uživatelské procedury* a ujistěte se, že jednotlivé zprávy jsou prověřeny pro autorizaci.

Zde je několik faktů o způsobu, jakým produkt IBM MQ for IBM i obsluhuje zabezpečení:



- Uživatelé jsou identifikováni a ověřeni produktem IBM i.
- Služby správce front vyvolané aplikacemi jsou spouštěny s oprávněním uživatelského profilu správce front, ale v rámci procesu uživatele.
- Služby správce front vyvolané příkazy uživatele jsou spuštěny s oprávněním uživatelského profilu správce front.

### **Zabezpečení objektů v systémech SYSTÉM UNIX a Linux**

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

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

### **ID uživatelů na systémech SYSTÉM UNIX a 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 na systémech Windows , pokud toto ID bude používat příkazy administrace produktu IBM MQ .

### **ID uživatelů na systémech Windows**

Pokud v systémech Windows *není-li instalována žádná uživatelská procedura pro zprávy*, bude správce front převeden na malá písmena nebo se smíšenými malými a velkými písmeny a velkými písmeny. Správce front poté vloží identifikátory uživatelů do kontextové části zprávy nebo zkontroluje jejich autorizaci. Oprávnění jsou proto založena pouze na identifikátorech malých písmen.

### **ID uživatelů v rámci systémů**

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

Chcete-li umožnit systému Windows, SYSTÉM UNIX a Linux používat malá písmena ve zprávách, provede na těchto platformách následující konverze:

#### **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 v systémech UNIX, Linux a Windows uvedete nějaký jiný důvod, automatické konverze se neprovedou.

### **Použití vlastní autorizační služby**

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

Komponenta autorizační služba dodaná s produktem IBM MQ se nazývá OAM (Object Authority Manager). Pokud produkt OAM neposkytuje potřebná oprávnění k autorizaci, můžete napsat vlastní komponentu autorizační služby. Instalovatelné funkce služby, které musí být implementovány komponentou autorizační služby, jsou popsány v tématu [Referenční informace o rozhraní instalovatelných služeb](#).

### **Řízení přístupu pro klienty**

Řízení přístupu je založeno na ID uživatelů. Pro správu může být mnoho ID uživatelů a ID uživatelů mohou být v různých formátech. Můžete nastavit vlastnost kanálu připojení serveru MCAUSER na speciální hodnotu ID uživatele, aby ji mohli používat klienti.

Řízení přístupu v produktu IBM MQ je založeno na ID uživatelů. ID uživatele procesu, který provádí volání MQI, se obvykle používá. Pro klienty MQ MQI je služba MCA pro připojení serveru znepřístupnila volání MQI pro klienty MQ MQI. Můžete vybrat alternativní ID uživatele pro produkt MCA připojení k serveru, který má být použit při vytváření volání MQI. Alternativní ID uživatele může být přidruženo buď k pracovní stanici klienta, nebo k tomu, co vyberete pro uspořádání a řízení přístupu klientů. ID uživatele musí mít k dispozici potřebná oprávnění, která jsou na serveru přidělena k vydávání volání MQI. Výběr alternativního ID uživatele je vhodnější, než umožníte klientům, aby učinili volání MQI s oprávněním agenta MCA připojení k serveru.

<i>Tabulka 9. ID uživatele použité kanálem připojení serveru</i>	
<b>Jméno uživatele</b>	<b>Při použití</b>
ID uživatele, které je nastaveno uživatelskou procedurou zabezpečení	Používá se, pokud není blokováno pravidlem <b>CHLAUTH TYPE (BLOCKUSER)</b> . Další informace najdete v následující sekci <a href="#">“Nastavení ID uživatele v uživatelské proceduře pro zabezpečení zprávy”</a> na stránce 85 .
ID uživatele, který je nastaven pravidlem CHLAUTH	Použije se, pokud není přepsáno uživatelskou procedurou zabezpečení. Další informace naleznete v tématu <a href="#">Záznamy ověřování kanálu</a> .
ID uživatele, které je definováno v atributu <b>MCAUSER</b> v definici kanálu SVRCONN	Používá se, pokud není přepsáno uživatelskou procedurou zabezpečení nebo pravidlem CHLAUTH.
ID uživatele, které je přenášeno z počítače klienta	Používá se, když žádné ID uživatele není nastaveno žádnými jinými prostředky.
ID uživatele, který spustil kanál připojení serveru	Používá se, když není žádné ID uživatele nastaveno žádnými jinými prostředky a žádné ID uživatele klienta není přenášeno. Další informace najdete v následující sekci <a href="#">“ID uživatele, který spouští program kanálu.”</a> na stránce 85 .

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 možnosti přístupu pro ID uživatele klienta. Tento přístup představuje řadu otázek, které je třeba vzít v úvahu:
  1. Pro ID uživatele na různých platformách existují různé formáty. To někdy způsobí problémy, pokud se formát ID uživatele na klientovi liší od přijatelných formátů na serveru.
  2. Existuje potenciálně mnoho klientů s různými a změna ID uživatelů. ID musí být definována a spravována na serveru.
  3. Je ID uživatele důvěryhodné? Libovolné ID uživatele může být tečeno z klienta, ne nutně ID přihlášeného uživatele. Klient může například proudit ID s úplným oprávněním mqm , které bylo záměrně definováno pouze na serveru z důvodů zabezpečení.
- Upřednostňovaný přístup je definovat tokeny identifikace klienta na serveru, a tak omezit schopnosti aplikací připojených ke klientovi. To se obvykle provádí nastavením vlastnosti kanálu připojení serveru MCAUSER na speciální hodnotu ID uživatele, které mají být použity klienty, a definování několika ID pro použití klienty s odlišnou úrovní autorizace na serveru.

## Nastavení ID uživatele v uživatelské proceduře pro zabezpečení zprávy

Pro produkt IBM MQ MQI clients 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.

Klient produktu IBM MQ nevyužívá při použití uživatelské procedury zabezpečení na straně klienta deklarovanou ID uživatele na server.

## ID uživatele, který spouští program kanálu.

Když jsou pole ID uživatele odvozena od ID uživatele, který spustil kanál připojení serveru, použije se tato hodnota:

- Pro produkt z/OS je ID uživatele přiřazeného ke spuštění úloze iniciátoru kanálu spuštěné v tabulce procedur spuštěných z/OS .
- Pro TCP/IP (non- z/OS ), ID uživatele z položky `inetd.conf` nebo ID uživatele, který spustil modul listener.
- Pro SNA (non- z/OS ), ID uživatele z položky serveru SNA nebo (pokud neexistuje) příchozí požadavek na připojení, nebo ID uživatele, který spustil modul listener.
- U protokolů NetBIOS a SPX ID uživatele, který spustil modul listener.

Pokud existují definice kanálu připojení serveru, které mají nastaven atribut MCAUSER na prázdnou hodnotu, klienti mohou tuto definici kanálu použít k připojení ke správci front s oprávněním pro přístup určeným ID uživatele dodaným klientem. Může se jednat o bezpečnostní riziko, pokud systém, v němž je správce front spuštěn, umožňuje neautorizované síťové připojení. Výchozí kanál připojení serveru IBM MQ (SYSTEM.DEF.SVRCONN) má atribut MCAUSER nastaven na prázdnou hodnotu. Chcete-li zabránit neoprávněnému přístupu, aktualizujte atribut MCAUSER výchozí definice se jménem uživatele, které nemá přístup k objektům produktu IBM MQ MQ .

## Velikost písmen ID uživatele

Definujete-li kanál pomocí `runmqsc`, změní se atribut MCAUSER na velká písmena, pokud se ID uživatele nevejde do jednoduchých uvozovek.

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

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

U serverů v systémech SYSTÉM UNIX a Linux je obsah pole `LongMCAUserIdentifier` obdrženy 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 86

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 91

*Ukončovací programy kanálu* jsou programy, které jsou volány v definovaných místech v posloupnosti zpracování agenta MCA. Uživatelé a dodavatelé mohou napsat své vlastní uživatelské programy kanálu. Některé jsou dodávány produktem IBM.

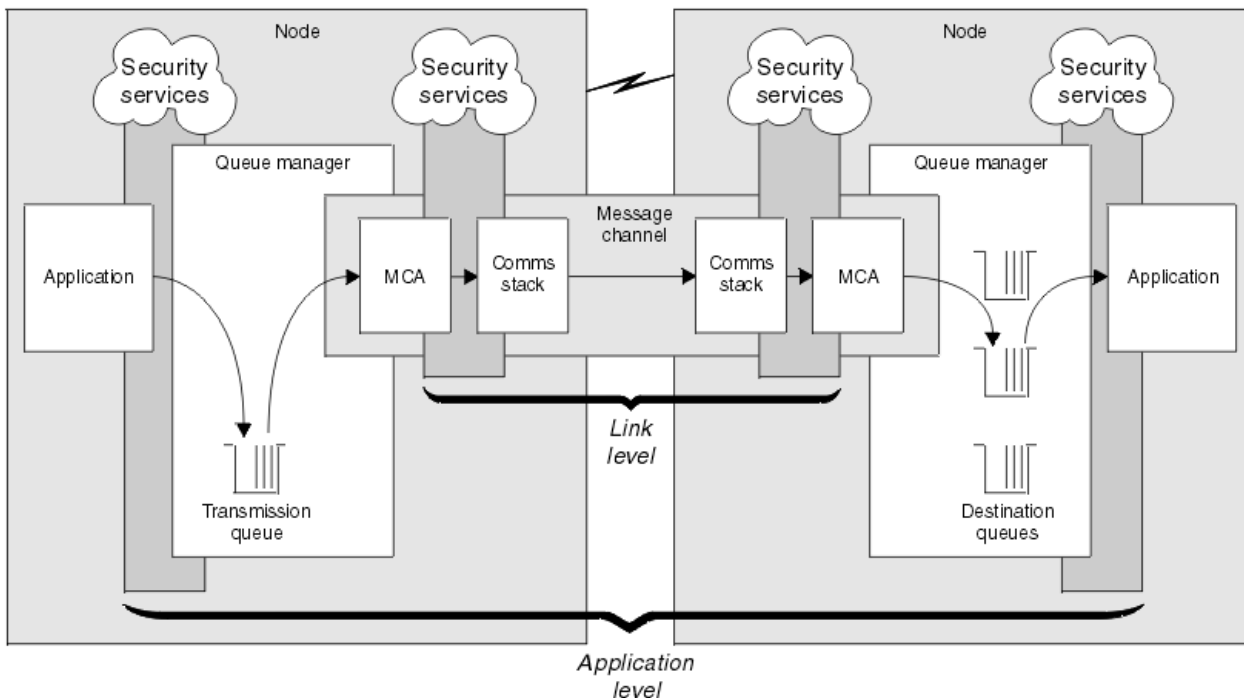
“Zabezpečení kanálů pomocí SSL/TLS” na stránce 97

Podpora TLS v produktu IBM MQ používá objekt ověřovacích informací správce front a různé příkazy MQSC. Musíte také zvážit použití digitálních certifikátů.

## Porovnání zabezpečení na úrovni odkazů a zabezpečení na úrovni aplikace

Toto téma obsahuje informace o různých aspektech zabezpečení na úrovni odkazů a zabezpečení na úrovni aplikací a porovnává dvě úrovně zabezpečení.

Úroveň odkazu a zabezpečení na úrovni aplikace jsou popsány v tématu Obrázek 10 na stránce 86.



Obrázek 10. Zabezpečení na úrovni odkazů a zabezpečení na úrovni aplikace

## Ochrana zpráv ve frontách

Zabezpečení na úrovni linky může chránit zprávy, zatímco jsou přenášeny z jednoho správce front do jiného. Je zvláště důležité, když jsou zprávy přenášeny přes nezabezpečenou síť. Nemůže však chránit zprávy, dokud jsou uloženy ve frontách buď ve zdrojovém správci front, v cílovém správci front, nebo ve středním správci front.

Zabezpečení na úrovni aplikace může díky porovnání chránit zprávy, zatímco jsou uloženy ve frontách a platí i v případě, že se nepoužívá distribuované řazení do fronty. To je hlavní rozdíl mezi úrovní

zabezpečení na úrovni zabezpečení a zabezpečení na úrovni aplikace a ilustrovat se v části [Obrázek 10 na stránce 86](#).

## **Správci front nejsou spuštěni v řízeném a důvěryhodném prostředí**

Je-li správce front spuštěn v řízeném a důvěryhodném prostředí, mohou být mechanismy řízení přístupu poskytované produktem IBM MQ považovány za dostatečné k ochraně zpráv uložených ve frontách. To platí zvláště v případě, že je zahrnuto pouze lokální řazení do fronty a zprávy nikdy neopustí správce front. Zabezpečení na úrovni aplikace v tomto případě může být považováno za zbytečné.

Zabezpečení na úrovni aplikace může být také považováno za zbytečné, pokud jsou zprávy přenášeny do jiného správce front, který je také spuštěn v řízeném a důvěryhodném prostředí, nebo jsou tyto zprávy přijaty od takového správce front. Potřeba zabezpečení na úrovni aplikace se stává větší, když jsou zprávy přenášeny nebo přijímány od správce front, který není spuštěn v řízeném a důvěryhodném prostředí.

## **Rozdíly v nákladech**

Zabezpečení na úrovni aplikace může stát více než zabezpečení na úrovni odkazů, pokud jde o administraci a výkon.

Náklady na administraci budou pravděpodobně větší, protože existují potenciálně více omezení pro konfiguraci a údržbu. Můžete například chtít zajistit, aby konkrétní uživatel odesílal pouze určité typy zpráv a odesílal zprávy pouze do určitých míst určení. A naopak, možná budete muset zajistit, aby určitý uživatel přijímal pouze určité typy zpráv a přijímal zprávy pouze z určitých zdrojů. Místo správy služeb zabezpečení na úrovni propojení na jednom kanálu zpráv může být třeba konfigurovat a spravovat pravidla pro každou dvojici uživatelů, kteří si vyměňují zprávy v rámci daného kanálu.

Je-li služba zabezpečení vyvolána pokaždé, když aplikace vloží nebo obdrží zprávu, může dojít k ovlivnění výkonu.

Organizace mají tendenci uvažovat o zabezpečení na úrovni odkazů jako první, protože by mohlo být jednodušší implementovat. Zváží zabezpečení na úrovni aplikace, pokud zjistí, že zabezpečení na úrovni odkazů nesplňuje všechny jejich požadavky.

## **Dostupnost komponent**

Obecně platí, že v distribuovaném prostředí služba zabezpečení vyžaduje komponentu na minimálně dvou systémech. Například, zpráva může být šifrována na jednom systému a dešifrována na jiném systému. To platí jak pro zabezpečení na úrovni odkazů, tak pro zabezpečení na úrovni aplikace.

V heterogenním prostředí s různými platformami, z nichž každá má různé úrovně zabezpečení, nemusí být požadované komponenty služby zabezpečení dostupné pro každou platformu, na které jsou potřeba, a v podobě, kterou lze snadno použít. Pravděpodobně se jedná o spíše problém zabezpečení na úrovni aplikace než zabezpečení na úrovni odkazů, a to zejména v případě, že máte v úmyslu poskytovat vlastní zabezpečení na úrovni aplikací prostřednictvím nákupu v komponentách z různých zdrojů.

## **Zprávy ve frontě nedoručených zpráv**

Je-li zpráva chráněna zabezpečení na úrovni aplikace, může dojít k problému, pokud zpráva z nějakého důvodu nedosáhne místa určení a je vložena do fronty nedoručených zpráv. Pokud nemůžete pracovat na tom, jak zpracovat zprávu z informací v deskriptoru zpráv a záhlaví zablokovaných dopisů, může být nutné zkontrolovat obsah dat aplikace. Tuto akci nelze provést, pokud jsou data aplikace šifrována a může ji dešifrovat pouze určený příjemce.

## **Co zabezpečení na úrovni aplikace nelze provést**

Zabezpečení na úrovni aplikace není kompletní řešení. I když implementujete zabezpečení na úrovni aplikací, můžete stále ještě vyžadovat některé služby zabezpečení na úrovni odkazů. Příklad:

- Když se spustí kanál, vzájemné ověření těchto dvou jednotek MCA může být stále ještě požadavek. To lze provést pouze pomocí služby zabezpečení na úrovni odkazu.

- Zabezpečení na úrovni aplikace nemůže ochránit záhlaví přenosové fronty, MQXQH, které obsahuje vložený deskriptor zprávy. Stejně tak nemůže chránit data v jiných tocích protokolu kanálu produktu IBM MQ než data zpráv. Tuto ochranu mohou poskytnout pouze zabezpečení na úrovni odkazů.
- Pokud jsou služby zabezpečení na úrovni aplikace vyvolány na konci kanálu serveru MQI, služby nemohou chránit parametry volání MQI, která jsou odesílána přes kanál. Data aplikací v rámci volání MQPUT, MQPUT1 nebo MQGET jsou však nechráněná. Ochranu může v tomto případě zajistit pouze zabezpečení na úrovni odkazů.

### ***zabezpečení na úrovni odkazů***

*Zabezpečení na úrovni odkazu odkazuje na tyto služby zabezpečení, které jsou přímo nebo nepřímo vyvolány agentem MCA, komunikačním subsystémem nebo kombinací těchto dvou činností.*

Zabezpečení na úrovni odkazu je ilustrováno v [Obrázek 10 na stránce 86](#).

Zde je několik příkladů služeb zabezpečení na úrovni odkazu:

- Agent MCA na každém konci kanálu zpráv může ověřit jeho partnera. To se provádí při spuštění kanálu a bylo ustanoveno komunikační spojení, ale před zahájením toku zpráv. Pokud dojde k selhání ověření na každém konci, kanál se zavře a žádné zprávy se nepřenášejí. Toto je příklad identifikace a ověřovací služby.
- Zprávu lze šifrovat na odesílající straně kanálu a dešifrována na přijímajícím konci. Toto je příklad služby důvěrnosti.
- Na přijímajícím konci kanálu může být zkontrolována zpráva s cílem určit, zda byl její obsah během přenosu po síti úmyslně změněn. Toto je příklad služby integrity dat.

### **Zabezpečení na úrovni odkazu poskytované produktem IBM MQ**

Primárním prostředkem pro zajištění důvěrnosti a integrity dat v produktu IBM MQ je použití zabezpečení SSL nebo TLS. Další informace o použití SSL a TLS v produktu IBM MQ viz [“Protokoly zabezpečení SSL a TLS v produktu IBM MQ” na stránce 22](#). Pro ověření poskytuje produkt IBM MQ zařízení k použití záznamů ověření kanálu. Záznamy ověření kanálu nabízejí přesnou kontrolu nad přístupem udělenou připojujícím se systémům na úrovni jednotlivých kanálů nebo skupin kanálů. Další informace viz [“Záznamy ověření kanálu” na stránce 48](#).

#### *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 91](#). Stejně téma také popisuje ukončovací program kanálu, který je dodáván s programem IBM MQ for Windows (uživatelským programem kanálu SSPI). Tento výstupní program kanálu je dodáván ve zdrojovém formátu, takže je možné upravit zdrojový kód tak, aby vyhovoval vašim požadavkům. Pokud tento výstupní program kanálu nebo výstupní programy kanálu dostupné od jiných dodavatelů nesplňují vaše požadavky, můžete navrhnout a napsat vlastní. Toto téma obsahuje návrhy způsobů, jak mohou uživatelské programy kanálu poskytovat služby zabezpečení. Informace o tom, jak zapisovat ukončovací program kanálu, najdete v tématu [Psaní programů ukončovacích programů](#).

#### *Zabezpečení na úrovni odkazu pomocí uživatelské procedury zabezpečení*

Uživatelské procedury zabezpečení normálně pracují ve dvojicích; jedna na každém konci kanálu. Zavolají se ihned po dokončení počátečního vyjednávání dat při spuštění kanálu.

Uživatelské procedury zabezpečení lze použít k poskytnutí identifikace a ověření, přístupu k řízení přístupu a důvěrnosti.

#### *Zabezpečení na úrovni odkazu pomocí uživatelské procedury pro zprávy*

Ukončení zprávy lze použít pouze v kanálu zpráv, nikoli v kanálu MQI. Má přístup k záhlaví přenosové fronty, MQXQH, které obsahuje vložený deskriptor zpráv, a data aplikace ve zprávě. Může upravovat obsah zprávy a měnit jeho délku.

Ukončení zprávy lze použít pro jakýkoli účel, který vyžaduje přístup k celé zprávě, spíše než její části.

Uživatelské procedury pro zprávy lze použít k poskytnutí identifikace a ověření, řízení přístupu, důvěrnosti, integrity dat a neodmítání, a z jiných důvodů než zabezpečení.

#### *Zabezpečení na úrovni odkazu pomocí uživatelských procedur pro odesílání a příjem*

Uživatelské procedury pro odesílání a příjem lze použít na obou zprávách i v kanálech MQI. Jsou volány pro všechny typy dat, které proudí na kanálu, a pro toky v obou směrech.

Uživatelské procedury pro odesílání a příjem mají přístup ke každému segmentu přenosu. Mohou upravovat jeho obsah a měnit jeho délku.

Pokud je v kanálu zpráv potřeba sběrnice MCA rozdělit zprávu a odeslat ji ve více než jednom segmentu přenosu, je volaná uživatelská procedura pro odeslání volána pro každý přenosový segment obsahující část zprávy a na přijímajícím konci je volána uživatelská procedura pro příjem pro každý segment přenosu. Pokud jsou vstupní nebo výstupní parametry volání MQI příliš velké na to, aby mohly být odeslány v rámci jednoho segmentu přenosu, dojde ke stejnému výsledku.

Na kanálu MQI označuje bajt 10 pro segment přenosu volání MQI a udává, zda segment přenosu obsahuje vstupní nebo výstupní parametry volání. Uživatelské procedury pro odesílání a příjem mohou zkoumat tento bajt a určit, zda volání MQI obsahuje data aplikací, která mohou být chráněna.

Je-li uživatelská procedura pro odeslání volána poprvé, získá a inicializuje všechny prostředky, které potřebuje, může požádat agenta MCA o vyhrazení zadaného množství prostoru ve vyrovnávací paměti, který obsahuje segment přenosu. Když je později volán ke zpracování segmentu přenosu, může použít tento prostor k přidání zašifrovaného klíče nebo digitálního podpisu, například. Odpovídající výstupní bod příjmu na druhém konci kanálu může odebrat data přidaná uživatelskou procedurou odeslání a použít ji ke zpracování segmentu přenosu.

Uživatelské procedury pro odesílání a příjem jsou nejvhodnější pro účely, v nichž nemusí rozumět struktuře dat, které zpracovávají, a mohou proto přistupovat ke každému segmentu přenosu jako s binárním objektem.

Uživatelské procedury pro odesílání a příjem lze použít k zajištění utajení a integrity dat a k použití jiných než zabezpečení.

#### **Související informace**

Identifikace volání rozhraní API v ukončovacím programu pro odeslání nebo přijetí

#### ***zabezpečení na úrovni aplikace***

*Zabezpečení na úrovni aplikace* odkazuje na ty služby zabezpečení, které jsou vyvolány na rozhraní mezi aplikací a správcem front, ke kterému je připojena.

Tyto služby jsou vyvolány, když aplikace odesílá volání MQI do správce front. Služby mohou být vyvolány přímo nebo nepřímo aplikací, správcem front, jiným produktem, který podporuje produkt IBM MQ, nebo kombinací libovolné z těchto pracovních procesů. Zabezpečení na úrovni aplikace je ilustrováno v tématu Obrázek 10 na stránce 86.

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

Pokud přesouváte vysoce citlivé nebo cenné informace, zejména důvěrné informace nebo informace související s platbami, jako jsou záznamy pacientů nebo podrobnosti o kreditní kartě, musíte věnovat zvláštní pozornost zabezpečení informací. Zajištění toho, aby byly informace pohybující se kolem podniku zachovány jeho integrity a chráněny před neoprávněným přístupem, je pokračující výzvou a zodpovědností. Pravděpodobně se budete muset řídit bezpečnostními předpisy, a to s rizikem sankcí za nedodržování norem.

Můžete vyvinout vlastní rozšíření zabezpečení na produkt IBM MQ. Tato řešení však vyžadují specializované dovednosti a mohou být složité a nákladné udržovat. Produkt IBM MQ Advanced Message Security pomáhá řešit tyto problémy při přesouvání informací v podniku prakticky ve všech typech komerčních informačních systémů.

Produkt IBM MQ Advanced Message Security rozšiřuje funkce zabezpečení produktu IBM MQ následujícími způsoby:

- Poskytuje ochranu dat na úrovni aplikací a koncových bodů pro infrastrukturu systému zpráv s cílem použít buď šifrování, nebo digitální podepisování zpráv.
- Poskytuje komplexní zabezpečení, aniž by bylo nutné psát komplexní kód zabezpečení nebo upravovat či opětovně kompilovat existující aplikace.
- Využívá technologii PKI (Public Key Infrastructure) k zajištění služeb ověření, autorizace, utajení a integrity dat pro zprávy.
- Poskytuje administraci zásad zabezpečení pro sálové počítače a distribuované servery.
- Podporuje jak IBM MQ servery, tak klienty.
- Poskytuje integraci s produktem IBM MQ Managed File Transfer pro poskytování řešení zabezpečeného systému zpráv typu end-to-end.

Další informace viz [“IBM MQ Advanced Message Security” na stránce 438.](#)

### *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 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 MQ .

Nejběžnější důvody použití rozhraní API vyšší úrovně jsou:

- Chcete-li skrýt rozšířené funkce rozhraní MQI od programátorů, postupujte takto:
- Chcete-li vynutit standardy při použití rozhraní MQI, postupujte takto:
- Přidání funkce do MQI. Tato dodatečná funkce může být službami zabezpečení.

Některé produkty dodavatelů používají tuto techniku k zajištění zabezpečení na úrovni aplikací pro produkt IBM MQ.

Plánujete-li poskytovat služby zabezpečení tímto způsobem, uvědomte si následující údaje týkající se konverze dat:

- Pokud byl do aplikační dat ve zprávě přidán token zabezpečení, jako je například digitální podpis, musí být jakýkoli kód provádějící převod dat vědom přítomnosti tohoto tokenu.

- Token zabezpečení mohl být odvozen z binárního obrazu dat aplikace. Proto každá kontrola tokenu musí být provedena před převodem dat.
- Pokud byla data aplikace ve zprávě šifrována, musí být dešifrována před převodem dat.

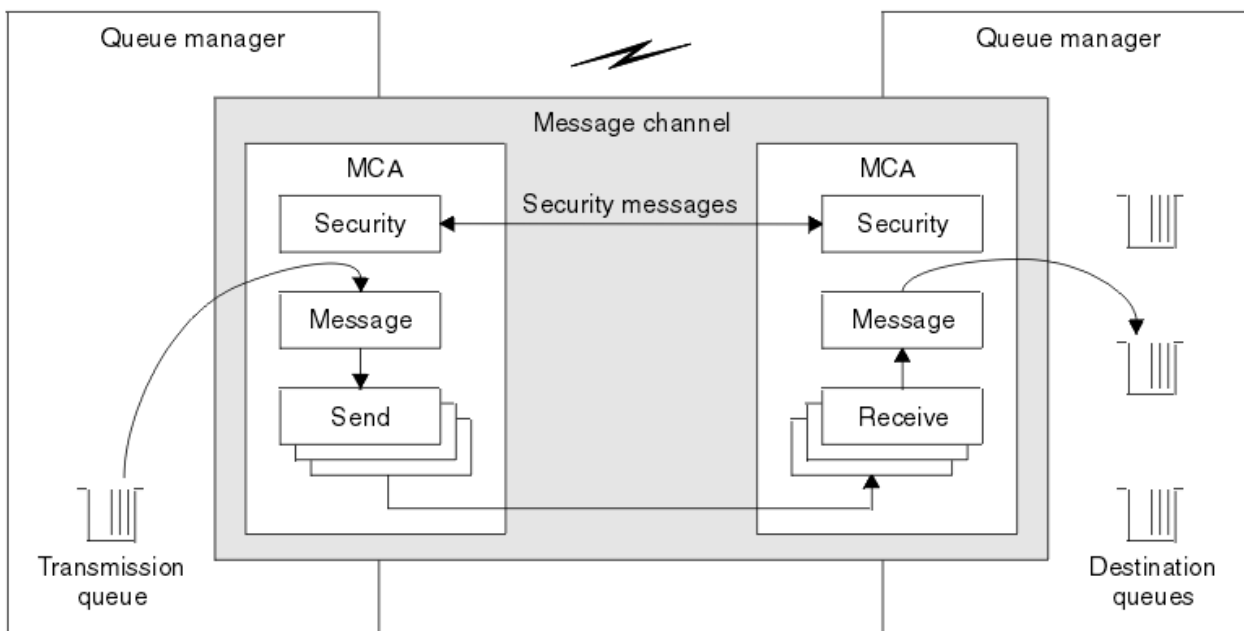
## Ukončovací programy kanálu

*Ukončovací programy kanálu* jsou programy, které jsou volány v definovaných místech v posloupnosti zpracování agenta MCA. Uživatelé a dodavatelé mohou napsat své vlastní uživatelské programy kanálu. Některé jsou dodávány produktem IBM.

Existuje několik typů ukončovacích programů kanálu, ale pouze čtyři mají roli při poskytování zabezpečení na úrovni odkazu:

- Uživatelská procedura pro zabezpečení zprávy
- Ukončení zprávy
- Ukončení odeslání
- Ukončení příjmu

Tyto čtyři typy ukončovacích programů kanálu jsou popsány v tématu Obrázek 11 na stránce 91 a jsou popsány v následujících tématech.



Obrázek 11. Uživatelské procedury zabezpečení, zprávy, odeslání a přijetí na kanálu zpráv

### Související informace

[Kanály-uživatelské programy pro kanály systému zpráv](#)

### Přehled uživatelské procedury zabezpečení

Uživatelské procedury zabezpečení normálně pracují ve dvojicích. Jsou volány před tokem zpráv a jejich účelem je umožnit agentovi MCA ověření jeho partnera.

*Uživatelské procedury zabezpečení* obvykle pracují ve dvojicích; jedna na každém konci kanálu. Jsou volány ihned po dokončení počátečního vyjednávání dat při spuštění kanálu, ale předtím, než začnou být odesílány zprávy. Primárním účelem uživatelské procedury zabezpečení je umožnit agentovi MCA na každém konci kanálu ověřovat jeho partnera. Avšak neexistuje nic, co by bránilo ukončení zabezpečení z provádění jiné funkce, dokonce i funkce, která nemá nic společného se zabezpečením.

Uživatelské procedury zabezpečení mohou vzájemně komunikovat odesláním *zpráv zabezpečení*. Formát zprávy zabezpečení není definován a je určován uživatelem. Jeden možný výsledek výměny zpráv

zabezpečení je takový, že jedna z uživatelských procedur zabezpečení může rozhodnout, že nebude pokračovat dále. V takovém případě je kanál uzavřen a zprávy nevedou k toku. Pokud existuje uživatelská procedura zabezpečení pouze na jednom konci kanálu, je tato uživatelská procedura stále volána a může se rozhodnout, zda má kanál pokračovat, nebo zavřít kanál.

Uživatelské procedury zabezpečení lze volat pro kanály zpráv i pro kanály MQI. Název uživatelské procedury zabezpečení je určen jako parametr v definici kanálu na každém konci kanálu.

Další informace o uživatelských procedurách zabezpečení najdete v tématu [“Zabezpečení na úrovni odkazu pomocí uživatelské procedury zabezpečení”](#) na stránce 88.

### **Ukončení zprávy**

Uživatelské procedury pro zprávy pracují pouze na kanálech zpráv a normálně pracují ve dvojicích. Ukončení zprávy může pracovat na celé zprávě a provádět na něm různé změny.

*Ukončení zpráv* na konci odesílání a přijímání konců kanálu obvykle pracuje ve dvojicích. Uživatelská procedura pro odeslání zprávy na odesílajícím konci kanálu je volána poté, co program MCA obdržel zprávu z přenosové fronty. Na přijímajícím konci kanálu je uživatelská procedura pro zprávy volána před tím, než agent MCA vloží zprávu do cílové fronty.

Uživatelská procedura pro zprávy má přístup k záhlaví přenosové fronty, MQXQH, které obsahuje vložený deskriptor zpráv, a data aplikace ve zprávě. Uživatelská procedura pro zprávy může upravit obsah zprávy a změnit jeho délku. Změna délky může být výsledkem komprimace, dekomprimace, šifrování nebo dešifrování zprávy. Může se také jednat o výsledek přidání dat do zprávy nebo o odebrání dat z ní.

Uživatelské procedury pro zprávy lze použít k jakémukoli účelu, který vyžaduje přístup k celé zprávě, nikoli jeho části, a ne nezbytně pro zabezpečení.

Ukončení zprávy může určit, že zpráva, kterou momentálně zpracovává, by neměla dále směřovat ke svému cíli. Agent MCA poté vloží zprávu do fronty nedoručených zpráv. Ukončení kanálu může také zavřít okno ukončení zprávy.

Uživatelské procedury pro zprávy lze volat pouze v kanálech zpráv, nikoli v kanálech MQI. Důvodem je to, že účelem kanálu MQI je povolit vstupní a výstupní parametry volání MQI pro tok mezi aplikací produktu IBM MQ MQI client a správcem front.

Název uživatelské procedury pro zprávy je určen jako parametr v definici kanálu na každém konci kanálu. Můžete také zadat seznam uživatelských procedur, které mají být spouštěny za dědění.

Další informace o uživatelských procedurách pro zprávy naleznete v tématu [“Zabezpečení na úrovni odkazu pomocí uživatelské procedury pro zprávy”](#) na stránce 88.

### **Odeslat a přijmout uživatelské procedury**

Uživatelské procedury pro odesílání a příjem obvykle pracují ve dvojicích. Pracují na převodových segmentech a nejlépe se používají tam, kde struktura dat, která zpracovává, není relevantní.

*Uživatelská procedura odeslání* na jednom konci kanálu a *uživatelská procedura příjmu* na druhém konci normálně pracují ve dvojicích. Uživatelská procedura pro odeslání zprávy je volána těsně před tím, než program MCA odešle oznámení o odeslání dat prostřednictvím komunikačního spojení. Uživatelská procedura pro příjem je volána bezprostředně poté, co agent MCA znovu získá řízení po přijetí komunikace a přijal data z komunikačního připojení. Je-li sdílení konverzací v použití kanálu MQI, je pro každou konverzaci volána jiná instance uživatelské procedury odeslání a přijetí.

Toky protokolu kanálu produktu IBM MQ mezi dvěma jednotkami MCAs v kanálu zpráv obsahují řídicí informace a také data zprávy. Podobně u kanálu MQI obsahují toky informace o řízení spolu s parametry volání MQI. Uživatelské procedury pro odesílání a příjem jsou volány pro všechny typy dat.

Data zprávy tečou pouze v jednom směru kanálu zpráv, ale na kanálu MQI se vstupní parametry toku volání MQI v jednom směru a výstupní parametry toku v druhém směru ubíjí. V případě kanálů zpráv i kanálů MQI lze řídit toky informací v obou směrech. V důsledku toho lze volat a přijímat uživatelské procedury na obou koncích kanálu.

Jednotka dat, která je přenášena v jednom toku mezi dvěma MCAs, se nazývá *transmission segment*. Uživatelské procedury pro odesílání a příjem mají přístup ke každému segmentu přenosu. Mohou

upravovat jeho obsah a měnit jeho délku. Uživatelská procedura odeslání však nesmí měnit prvních 8 bajtů segmentu přenosu. Těchto 8 bajtů tvoří část záhlaví protokolu kanálu IBM MQ . Existují také omezení, jak velká uživatelská procedura pro odeslání může zvýšit délku přenosového segmentu. Zejména odeslání uživatelské procedury odeslání nemůže zvýšit svou délku nad maximum, které bylo vyjednáno 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, MQPUT1 nebo MQGET, pokud jsou data aplikace dostatečně velká.

Vezmeme-li tyto úvahy v úvahu, je vhodnější použít pro účely odeslání a přijetí uživatelské procedury, které nepotřebují rozumět struktuře dat, které zpracovávají, a mohou proto přistupovat ke každému segmentu přenosu jako k binárnímu objektu.

Odesílatel nebo přijímací procedura může zavřít kanál.

Názvy uživatelské procedury odeslání a ukončení příjmu jsou uvedeny jako parametry v definici kanálu na každém konci kanálu. Můžete také uvést seznam uživatelských procedur odeslání, které mají být spuštěny v posloupnosti. Podobně můžete zadat seznam ukončení příjmu.

Další informace o uživatelských procedurách pro odesílání a příjem naleznete v příručce [“Zabezpečení na úrovni odkazu pomocí uživatelských procedur pro odesílání a příjem”](#) na stránce 89.

## Plánování integrity dat

Naplánujte, jak zachovat integritu vašich dat.

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

Na úrovni aplikace můžete použít výstupní programy rozhraní API, pokud standardní zařízení nevyhovují vašim požadavkům. Můžete se rozhodnout použít produkt IBM MQ Advanced Message Security (AMS) k digitálnímu podpisu zpráv za účelem ochrany proti neautorizované úpravě.

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

[“Zabezpečení kanálů pomocí SSL/TLS”](#) na stránce 97

Podpora TLS v produktu IBM MQ používá objekt ověřovacích informací správce front a různé příkazy MQSC. Musíte také zvážit použití digitálních certifikátů.

[“Integrita dat v produktu IBM MQ”](#) na stránce 22

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

[“Plánování pro databázi Advanced Message Security”](#) na stránce 90

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

### Související informace

[Popis uživatelské procedury rozhraní](#)

[Volání uživatelských procedur kanálů a datové struktury](#)

## Plánování monitorování

Rozhodněte se, která data budete potřebovat k monitorování, a jak zachytíte a zpracujete informace o auditu. Zvažte, jak zkontrolovat, zda je systém správně nakonfigurovaný.

Existuje několik aspektů monitorování aktivity. Aspekty, které musíte vzít v úvahu, jsou často definovány požadavky auditora, a tyto požadavky jsou často řízeny regulačními standardy, jako jsou HIPAA (Health Insurance Portability and Accountability Act) nebo SOX (Sarbanes-Oxley). Produkt IBM MQ poskytuje funkce určené k pomoci s dodržováním těchto standardů.

Zvažte, zda máte zájem pouze o výjimky nebo o to, zda se zajímáte o veškeré chování systému.

Některé aspekty auditu lze také považovat za provozní monitorování; jedno rozlišování pro audit je takové, že se často díváte na historická data, nejen při pohledu na výstrahy v reálném čase. Monitorování je zahrnuto v sekci [Monitorování a výkon](#).

### Jaká data se mají monitorovat

Zvažte, jaké typy dat nebo činností je třeba monitorovat, jak je popsáno v následujících sekcích:

#### Změny provedené v produktu IBM MQ pomocí rozhraní produktu IBM MQ

Konfigurujte produkt IBM MQ, chcete-li vydat události přípravy nástrojů, zejména události příkazů a události konfigurace.

#### Změny provedené v produktu IBM MQ mimo jeho ovládací prvek

Některé změny mohou ovlivnit chování produktu IBM MQ, ale nelze je přímo monitorovat produktem IBM MQ. Příklady takových změn zahrnují změny v konfiguračních souborech `mqqs.ini`, `qm.inia` a `mqclient.ini`, vytváření a odstraňování správců front, instalaci binárních souborů, jako jsou uživatelské programy, a změny oprávnění k souboru. Chcete-li monitorovat tyto aktivity, musíte použít nástroje spuštěné na úrovni operačního systému. Jsou k dispozici různé nástroje a jsou vhodné pro různé operační systémy. Můžete také mít protokoly vytvořené přidruženými nástroji, jako je například `sudo`.

#### Provozní řízení IBM MQ

Je možné, že budete muset použít nástroje operačního systému k monitorování aktivit, jako je spouštění a zastavování správců front. V některých případech může být produkt IBM MQ nakonfigurován k vydávání událostí přípravy nástrojů.

#### Aktivita aplikace v rámci produktu IBM MQ

Chcete-li monitorovat akce aplikací, například otevírání front a vkládání zpráv a získávání zpráv, nakonfigurujte produkt IBM MQ tak, aby vydal odpovídající události.

#### Výstrahy nepravdivosti

Chcete-li provést audit při pokusu o narušení zabezpečení, nakonfigurujte systém tak, aby vydal události autorizace. Události kanálu mohou být užitečné také k zobrazení aktivity, zvláště pokud je kanál neočekávaně ukončen.

## Plánování zachytávání, zobrazení a archivace dat auditu

Řadu z prvků, které potřebujete, jsou nahlášeny jako zprávy událostí produktu IBM MQ. Musíte vybrat nástroje, které mohou tyto zprávy číst a formátovat. Pokud se zajímáte o dlouhodobé uložení a analýzu, musíte je přesunout do pomocného úložného mechanismu, jako je například databáze. Pokud tyto zprávy nezpracovávají, zůstanou ve frontě událostí a pravděpodobně budou zaplňovat frontu. Můžete se rozhodnout implementovat nástroj, který automaticky provede akce na základě některých událostí; chcete-li například vydat výstrahu, dojde-li k selhání zabezpečení.

### Ověření, že je systém správně nakonfigurován

Sada testů se dodává spolu s MQ Explorer. Použijte tyto informace ke kontrole problémů v definicích objektů.

Také pravidelně kontrolujte, že konfigurace systému je taková, jakou očekáváte. Ačkoli může příkaz a události konfigurace hlásit, kdy se něco změnilo, je také užitečné vypsát konfiguraci a porovnat ji se známou dobrou kopií.

## Plánování zabezpečení podle topologie

Tento oddíl se zabývá zabezpečením ve specifických situacích, konkrétně pro kanály, klastry správců front, aplikace publikování/odběru a výběrového vysílání a při použití brány firewall.

Další informace naleznete v následujících dílčích tématech:

### Ověřování kanálu

Pokud odešlete nebo obdržíte zprávu prostřednictvím kanálu, musíte poskytnout přístup k různým prostředkům produktu IBM MQ . Agenti MCA (Message Channel Agents) jsou v podstatě IBM MQ aplikace, které přesouvají zprávy mezi správci front a jako takové vyžadují přístup k různým prostředkům produktu IBM MQ , aby fungovaly správně.

Chcete-li přijímat zprávy v čase PUT pro MCA, můžete použít buď ID uživatele přidružené k agentovi MCA, nebo ID uživatele přidružené ke zprávě.

V čase CONNECT můžete namapovat ID uživatele na alternativního uživatele pomocí ověřovacích záznamů kanálu produktu **CHLAUTH** .

V produktu IBM MQ mohou být kanály chráněny pomocí TLS podpory.

ID uživatelů přidružená k odesílání a přijímání kanálů, kromě odesílacího kanálu, kde je atribut MCAUSER nepoužívaný, vyžaduje přístup k následujícím prostředkům:

- ID uživatele přidružené k odesílacímu 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 přijímacím kanálem můžete otevřít cílové fronty pro vkládání zpráv do front.

To zahrnuje rozhraní MQI (Message Queuing Interface), takže mohou být provedeny další kontroly řízení přístupu, pokud nepoužíváte produkt IBM MQ Object Authority Manager (OAM).

Můžete uvést, zda jsou kontroly autorizace provedeny proti ID uživatele přidruženému ke zprávě MCA (jak je popsáno v tomto tématu), nebo proti ID uživatele přidruženému ke zprávě (z pole MQMD [UserIdentifier](#) ).

U typů kanálů, na které se vztahuje, určuje parametr **PUTAUT** definice kanálu, které ID uživatele se použije pro tyto kontroly.

- Výchozí nastavení kanálu je použití účtu služby správce front, který 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.



- **V 8.0.0.4** Pokud před Verze 8.0.0, opravná sada 4použijete ID uživatele, které nemá oprávnění k administraci produktu IBM MQ , musíte pro kanál k práci udělit oprávnění **dsp** a **ctrlx** pro kanál k tomuto ID uživatele.

V produktu Verze 8.0.0, opravná sada 4neexistují žádné kontroly oprávnění, když se kanál znovu synchronizuje a opravuje pořadová čísla.

Nicméně zadání příkazu RESET CHANNEL ručně stále vyžaduje **+dsp** a **+ctrlx** ve všech vydáních.



**Upozornění:** Je-li pro potvrzení dávky zpráv zapotřebí resetování kanálu, produkt IBM MQ se pokusí o dotaz na kanál, který vyžaduje oprávnění správce **+dsp** .

- Atribut MCAUSER se nepoužívá pro typ kanálu SDR.
- Použijete-li ID uživatele přidružené ke zprávě, je pravděpodobné, že ID uživatele pochází ze vzdáleného systému.

Toto ID uživatele vzdáleného systému musí být rozpoznáno cílovým systémem. 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 nadřazenému 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 48](#)



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

### **Související informace**

[Vlastnosti záznamu ověření kanálu](#)

### **Zabezpečení definic inicializátoru kanálu**

Inicializátory inicializátorů kanálu mohou manipulovat pouze členové skupiny mqm.

Inicializátory kanálu produktu IBM MQ nejsou objekty produktu IBM MQ ; přístup k nim není řízen produktem OAM. Produkt IBM MQ neumožňuje uživateli 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 vložit zprávu přímo do přenosové fronty, vyžaduje to zvláštní oprávnění; viz [Tabulka 12 na stránce 121](#).

### **Uživatelské procedury kanálu**

Nejsou-li záznamy ověření kanálu vhodné, můžete pro přidání 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 91 .

### **Zabezpečení kanálů pomocí SSL/TLS**

Podpora TLS v produktu IBM MQ používá objekt ověřovacích informací správce front a různé příkazy MQSC. Musíte také zvážit použití digitálních certifikátů.

### **Digitální certifikáty a klíčová úložiště**

Dobrým zvykem je nastavit atribut návěští certifikátu správce front ( **CERTLABL** ) na název osobního certifikátu, který má být použit pro většinu kanálů, a přepsat jej pro výjimky tím, že nastavíte jmenovku certifikátu na těchto kanálech, které vyžadují různé certifikáty.

Potřebujete-li mnoho kanálů s certifikáty, které se liší od výchozího nastavení certifikátů ve správci front, měli byste zvážit rozdělení kanálů mezi několik správců front nebo použít server proxy MQIPT před správcem front za účelem předložení jiného certifikátu.

Pro každý kanál můžete použít jiný certifikát, ale pokud ukládáte příliš mnoho certifikátů v úložišti klíčů, můžete očekávat, že bude mít vliv na výkon při spouštění kanálů TLS. Pokuste se zachovat počet certifikátů v úložišti klíčů méně než přibližně 50 a považujte 100 za maximum, protože se výkon sady GSKit výrazně sníží s většími klíčovými úložišti.

Povolení více certifikátů ve stejném správci front zvyšuje pravděpodobnost, že bude ve stejném správci front použito více certifikátů CA. To zvyšuje pravděpodobnost, že obor názvů rozlišujícího názvu certifikátu koliduje s certifikáty vydanými oddělenými certifikačními autoritami.

Zatímco profesionální certifikační autority jsou pravděpodobně opatrnější, interní certifikační autority často postrádají jasné konvence pojmenování a vy byste mohli skončit nezamýšlenými shodami mezi CA a jinou CA.

Kromě rozlišujícího názvu subjektu byste měli zkontrolovat rozlišující název vydavatele certifikátu. Chcete-li tak učinit, použijte ověření kanálu SSLPEERMAP a nastavte pole **SSLPEER** i **SSLCERTI** tak, aby se shodovaly s DN subjektu a DN vydávajícího.

## Certifikáty podepsané svým držitelem a certifikáty podepsané (CA)

Je důležité naplánovat použití digitálních certifikátů, a to jak při vývoji a testování vaší aplikace, tak i pro její použití při výrobě. V závislosti na použití správců front a klientských aplikací můžete použít certifikáty podepsané CA nebo certifikáty s vlastním podpisem.

### Certifikáty podepsané (CA)

V případě produkčních systémů získáte 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:

**ULW** V systémech Windows, UNIXa Linux můžete používat certifikáty s vlastním podpisem. Pokyny naleznete v příručce “Vytvoření osobního certifikátu podepsaného sebou samým na serveru SYSTÉM UNIX, Linuxa Okna” na stránce 281.

**IBM i** V systému IBM i můžete používat certifikáty podepsané lokálním CA. Pokyny naleznete v příručce “Požádání o certifikát serveru v systému IBM i” na stránce 266 .

**z/OS** V systému z/OS můžete použít buď certifikáty podepsané sebou samým, nebo lokální certifikáty podepsané CA. Pokyny naleznete v příručce “Vytvoření osobního certifikátu podepsaného sebou samým na serveru z/OS” na stránce 308 nebo “Požádání o osobní certifikát v systému z/OS” na stránce 308 .

Certifikáty podepsané svým držitelem nejsou vhodné pro provozní účely, a to z těchto důvodů:

- Certifikáty podepsané sebou samým nelze odvolat, což může útočnickovi umožnit, aby po poškození soukromého klíče zanechal totožnost identity. Certifikační úřady mohou odvolat kompromitovaný certifikát, který zabrání jeho dalšímu použití. Certifikáty podepsané certifikační autoritou jsou proto bezpečnější pro použití v produkčním prostředí, ačkoli certifikáty podepsané sebou samým pro testovací systém jsou pohodlnější.
- Platnost certifikátů podepsaných sebou samým nikdy nevyprší. To je výhodné i bezpečné v testovacím prostředí, ale v produkčním prostředí je ponechá otevřené pro případné narušení zabezpečení. Riziko je znásobeno skutečností, že certifikáty podepsané sebou samým nelze odvolat.
- Certifikát s automatickým podpisem se používá jako osobní certifikát i jako kořenový certifikát CA (nebo jeho kotva důvěryhodnosti). Uživatel s osobním certifikátem podepsaným sebou samým by mohl být schopen jej použít k podepisování jiných osobních certifikátů. Obecně platí, že to neplatí pro osobní certifikáty vydané certifikačním úřadem a představují významnou expozici.

## CipherSpecs a digitální certifikáty

U všech podporovaných typů digitálních certifikátů lze použít pouze podmnožinu podporovaných CipherSpecs . Je proto nezbytné zvolit příslušnou CipherSpec pro vaše digitální certifikáty. Podobně platí, že pokud vaše zásada zabezpečení vaší organizace vyžaduje použití určité CipherSpec , je třeba získat vhodné digitální certifikáty.

Další informace o vztahu mezi CipherSpecs a digitálními certifikáty viz “Digitální certifikáty a kompatibilita CipherSpec v produktu IBM MQ” na stránce 44

## Zásady ověření platnosti certifikátu

Standard IETF RFC 5280 uvádí řadu pravidel pro ověření platnosti certifikátu, které musí implementovat vyhovující aplikační software, aby se zabránilo útokům zosobnění. Sada pravidel pro ověření platnosti certifikátu je známá jako zásada ověření platnosti certifikátu. Další informace o zásadách ověření platnosti

certifikátů v produktu IBM MQ naleznete v tématu [“Zásady ověření platnosti certifikátu v produktu IBM MQ”](#) na stránce 43.

## Plánování kontroly odvolání certifikátů

Povolení více certifikátů z různých certifikačních autorit může potenciálně způsobit zbytečnou další kontrolu odvolání certifikátů.

Konkrétně, pokud jste explicitně nakonfigurovali použití serveru pro odvolání z určité CA, například pomocí objektu AUTHINFO nebo struktury záznamu ověřovacích informací (MQAIR), kontrola odvolání selže, když se předkládá s certifikátem od jiného CA.

Měli byste se vyhnout explicitní konfiguraci serveru odvolaných certifikátů (CRL). Místo toho byste měli povolit implicitní kontrolu, kdy každý certifikát obsahuje vlastní umístění serveru odvolání v rozšíření certifikátu, například v distribučním bodu CRL nebo OCSP AuthorityInfoAccess.

Další informace viz [OCSPCheckExtensions](#) a [CDPCheckExtensions](#).

## Příkazy a atributy pro podporu TLS

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

- Následující příkazy MQSC podporují TLS:

### **ZMĚNIT AUTHINFO**

Upraví atributy objektu ověřovacích informací.

### **DEFINOVAT AUTHINFO**

Vytvoří objekt ověřovacích informací.

### **ODSTRANIT AUTHINFO**

Odstraní objekt ověřovacích informací.

### **ZOBRAZIT AUTHINFO**

Zobrazí atributy pro specifický objekt ověřovacích informací.

- Následující parametry správce front podporují TLS:

### **CERTLABL**

Definuje jmenovku osobního certifikátu, který má být použit.

### **SSLCRLNL**

Atribut SSLCRLNL uvádí seznam názvů objektů ověřovacích informací, které se používají k poskytnutí umístění odvolaných certifikátů k povolení rozšířené kontroly certifikátu TLS.

### **SSLCRYP**

V systémech Windows, SYSTÉM UNIX a 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 TLS hlášena v případě, že kanál, který používá TLS, nemůže vytvořit připojení TLS.

### **SSLFIPS**

Určuje, zda mají být použity pouze algoritmy certifikované podle standardu FIPS, pokud je šifrování prováděno v produktu IBM MQ, nikoli v kryptografickém hardwaru. Je-li konfigurován kryptografický hardware, jsou použity kryptografické moduly poskytované hardwarovým produktem a tyto šifrovací moduly mohou být certifikovány podle standardu FIPS na konkrétní úroveň. Závisí na tom, který hardware se používá.

## **SSLKEYR**

V systémech SYSTÉM UNIX, Linuxu Okna asociuje úložiště klíčů se správcem front. Databáze klíčů je zadržena v databázi klíčů *GSKit*. Produkt IBM Global Security Kit (GSKit) umožňuje používat zabezpečení TLS v systémech Windows, SYSTÉM UNIX a Linux.

## **SSLRKEYC**

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

- Následující parametry kanálu podporují TLS:

## **CERTLABL**

Definuje jmenovku osobního certifikátu, který má být použit.

## **SSLCAUTH**

Definuje, zda produkt IBM MQ vyžaduje a ověřuje certifikát od klienta TLS.

## **SSLCIPH**

Určuje sílu šifrování a funkci (CipherSpec), například `TLS_RSA_WITH_AES_128_CBC_SHA`. Shoda CipherSpec musí odpovídat oběma konci kanálu.

## **SSLPEER**

Uvádí rozlišující název (jedinečný identifikátor) povolených partnerů.

Tento oddíl popisuje příkazy **setmqaut**, **dspmqaut**, **dmpmqaut**, **rcrmqobj**, **rcdmqimg** a **dspmqfls** pro podporu objektu ověřovacích informací. Popisuje také příkaz **runmqckm** (iKeycmd) pro správu certifikátů v systémech SYSTÉM UNIX a Linux a nástroj **runmqakm** pro správu certifikátů v systému SYSTÉM UNIX, Linuxu Okna. Viz následující sekce:

- [setmqaut](#)
- [dspmqaut](#)
- [dmpmqaut](#)
- [rcrmqobj](#)
- [rcdmqimg](#)
- [dspmqfls](#)
- [Správa klíčů a certifikátů](#)

Přehled zabezpečení kanálu pomocí protokolu TLS naleznete v části

- [“Protokoly zabezpečení SSL a TLS v produktu IBM MQ” na stránce 22](#)

Podrobnosti o příkazech MQSC přidružených k protokolu TLS naleznete v

- [ALTER AUTHINFO](#)
- [Příkaz DEFINE AUTHINFO](#)
- [ODSTRANIT AUTHINFO](#)
- [ZOBRAZIT AUTHINFO](#)

Podrobnosti o příkazech PCF přidružených k protokolu TLS najdete v tématu

- [Změnit, kopírovat a vytvořit objekt ověřovacích informací](#)
- [Odstranit objekt ověřovacích informací](#)
- [Dotaz na objekt ověřovacích informací](#)

## **IBM MQ for z/OS Kanál připojení serveru**

Kanál SVRCONN produktu IBM MQ for z/OS není zabezpečen bez implementace ověřování kanálu nebo při přidávání uživatelské procedury zabezpečení s použitím zabezpečení SSL nebo protokolu TLS. Kanály SVRCONN nemají při výchozím nastavení zabezpečení definovanou jako výchozí.

## Bezpečnostní otázky

Kanály SVRCONN nejsou zabezpečené jako původně definované, SYSTEM.DEF.SVRCONN například. Chcete-li zabezpečit kanál SVRCONN, musíte nastavit ověření kanálu pomocí příkazu SET CHLAUTH nebo instalovat proceduru zabezpečení a implementovat SSL, nebo TLS.

Musíte použít veřejně dostupnou uživatelskou proceduru pro zabezpečení zprávy, napsat uživatelskou proceduru zabezpečení nebo zakoupit uživatelskou proceduru pro zabezpečení zprávy.

K dispozici je několik ukázek, které můžete použít jako dobrý počáteční bod pro zápis vlastního výstupního bodu zabezpečení kanálu SVRCONN.

V produktu IBM MQ for z/OS je člen CSQ4BCX3 ve vaší knihovně hlq.SCSQC37S ukázkou uživatelské procedury zabezpečení napsanou v jazyce C. Ukázka CSQ4BCX3 se také dodává předkompilovaným ve vaší knihovně hlq.SCSQAUTH .

Ukázkovou uživatelskou proceduru CSQ4BCX3 můžete implementovat zkopírováním kompilovaného členu hlq.SCSQAUTH(CSQ4BCX3) do zaváděcí knihovny, která je přidělena k CSQXLIB DD ve vašem CHIN Proc. Všimněte si, že CHIN vyžaduje, aby zaváděcí knihovna byla nastavena jako "Program Controlled".

Upravte kanál SVRCONN, aby nastavil CSQ4BCX3 jako uživatelskou proceduru pro zabezpečení zprávy.

Když se klient připojí pomocí daného kanálu SVRCONN, CSQ4BCX3 se bude ověřovat pomocí dvojice RemoteUserIdentifier a RemotePassword z MQCD. Je-li ověření úspěšné, zkopíruje identifikátor RemoteUserdo MCAUserIdentifier, změní kontext identity podprocesu.

Pokud napíšete klienta MQ Java , můžete použít popup k dotazování uživatele a nastavení MQEnvironment.userID a MQEnvironment.password. Tyto hodnoty budou předány při vytvoření připojení.

Nyní, když máte funkční uživatelskou proceduru zabezpečení, existuje další obava, že jméno uživatele a heslo jsou přenášeny jako prostý text po síti, když je vytvořeno připojení, stejně jako obsah všech následných zpráv produktu MQ . K šifrování těchto počátečních informací o připojení a obsahu všech zpráv MQ můžete použít SSL.

## Příklad

Chcete-li zabezpečit kanál SVRCONN MQ Explorer , SYSTEM.ADMIN.SVRCONN proveďte následující kroky:

1. Zkopírujte soubor hlq.SCSQAUTH(CSQ4BCX3) do zaváděcí knihovny, která je přidělena k CSQXLIB DD v CHINIT Proc.
2. Ověřte, že knihovna zavedení je Kontrolovaná programem.
3. Upravte SYSTÉM ADMIN.SVRCONN , aby používal proceduru zabezpečení CSQ4BCX3.
4. V produktu MQ Explorer klepněte pravým tlačítkem myši na název správce front produktu z/OS , vyberte volbu **Podrobnosti připojení > Vlastnosti > ID uživatele** a zadejte ID uživatele produktu z/OS .
5. Připojte se ke správci front produktu z/OS zadáním hesla.

## Další informace

Aby bylo možné ukončit program CSQ4BCX3 v prostředí s řízenými programy, vše načtené do adresního prostoru CHIN musí být zavedeno z knihovny řízené programem, například všechny knihovny v knihovně STEPLIB a všechny knihovny pojmenované na CSQXLIB DD. To set a load library as Program Controlled issue RACF commands. V následujícím příkladu je název knihovny načtení MY.TEST.LOADLIB.

```
RALTER PROGRAM * ADDMEM('MY.TEST.LOADLIB'//NOPADCHK)
SETROPTS WHEN(PROGRAM)REFRESH
```

Chcete-li změnit kanál SVRCONN za účelem implementace rozhraní CSQ4BCX3, zadejte následující příkaz MQ :

```
ALTER CHANNEL( SYSTEM ADMIN.SVRCONN) CHLTYPE(SVRCONN) SECYEXIT(CSQ4BCX3)
```

Ve výše uvedeném příkladu se používá název kanálu SVRCONN SYSTEM ADMIN.SVRCONN.

Další informace o uživatelských procedurách kanálu naleznete v příručce [“Ukončovací programy kanálu”](#) na stránce 91 .

### **Související informace**

[Zápis ukončovacích programů kanálu v systému z/OS](#)

## **Služby zabezpečení architektury SNA LU 6.2**

LU technologie SNA 6.2 nabízí šifrování na úrovni relace, ověření na úrovni relace a ověřování na úrovni konverzace.

**Poznámka:** Tato kolekce témat předpokládá, že máte základní informace o architektuře SNA (Systems Network Architecture). Druhá dokumentace uvedená v tomto oddílu obsahuje stručné úvodní informace o příslušných konceptech a terminologii. Požadujete-li komplexnější technický úvod do SNA, prostudujte si téma *Systems Network Architecture Technical Overview*, GC30-3073.

Logická jednotka SNA 6.2 poskytuje tři bezpečnostní služby:

- Šifrování na úrovni relace
- Ověření úrovně relace
- Ověření úrovně konverzace

V případě šifrování na úrovni relace a ověřování na úrovni relace používá SNA algoritmus *Data Encryption Standard (DES)*. Algoritmus DES je algoritmus šifry bloku, který používá symetrický klíč pro šifrování a dešifrování dat. Oba blok i klíč mají délku 8 bajtů.

### *Šifrování na úrovni relace*

*Šifrování na úrovni relace* šifruje a dešifruje data relací pomocí algoritmu DES. Lze jej proto použít k zajištění služby utajení na úrovni odkazů na kanálech LU SNA LU 6.2 .

Logické jednotky (LU) mohou poskytovat povinná (nebo požadovaná) šifrování dat, selektivní šifrování dat nebo žádné šifrování dat.

Na *povinném kryptografickém relacilogická* jednotka šifruje všechny odchozí jednotky požadavků na data a dešifruje všechny jednotky příchozích požadavků na data.

Na *výběrové šifrovací relaci* šifruje jednotka LU pouze jednotky dat požadavku zadané odesílajícím transakčním programem (TP). Odesílající LU signalizuje, že data jsou šifrována nastavením indikátoru v záhlaví požadavku. Zaškrtnutím tohoto indikátoru může přijímající logická jednotka zjistit, které jednotky mají být dešifrovány před jejich předáním do přijímajícího transakčního protokolu.

V síti SNA jsou to transakční programy IBM MQ MCAs. MCAs nepožaduje šifrování pro žádná data, která odesílají. Výběrové šifrování dat není proto volbou; v relaci je možné pouze povinné šifrování dat nebo žádné šifrování dat.

Informace o tom, jak implementovat povinné šifrování dat, najdete v dokumentaci k subsystému SNA. Další informace o silnějších formách šifrování, které mohou být k dispozici pro použití na platformě, jako je Triple DES 24bajtové šifrování na serveru z/OS, najdete v příslušné dokumentaci.

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

### *Ověření úrovně relace*

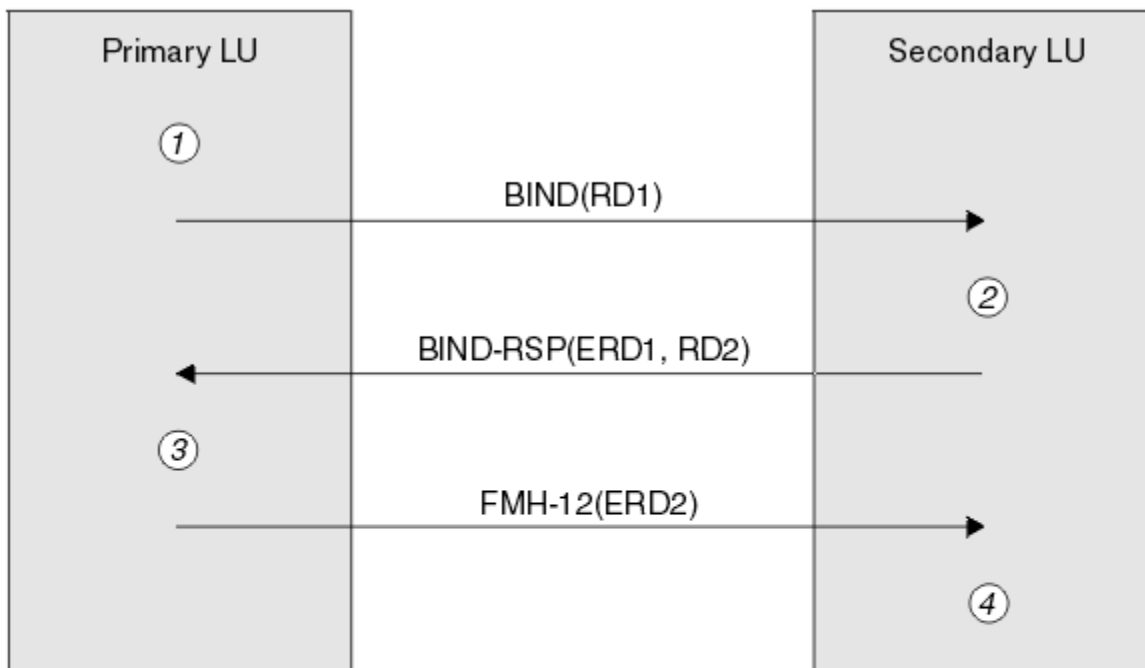
*Ověření úrovně relace* je protokol zabezpečení na úrovni relace, který umožňuje dvěma jednotkám LU, aby se navzájem ověřovali, zatímco aktivují relaci. Je také známý jako *Verifikace LU-LU*.

Vzhledem k tomu, že logická jednotka je ve skutečnosti "brána" do systému ze sítě, můžete tuto úroveň ověření považovat za dostatečné za určitých okolností. Pokud například správce front potřebuje vyměnit zprávy se vzdáleným správcem front, který je spuštěn v řízeném a důvěryhodném prostředí, můžete být

přípravě důvěřovat identitám zbývajících komponent vzdáleného systému po ověření logické jednotky LU.

Ověření úrovně relace je dosaženo každou LU, která ověřuje heslo svého partnera. Heslo se nazývá *heslo LU-LU*, protože jedno heslo se ustanoví mezi každou dvojicí jednotek LU. Způsob, jakým je vytvořeno heslo LU-LU, závisí na implementaci a mimo rozsah SNA.

Obrázek 12 na stránce 103 ilustruje toky pro ověření na úrovni relace.



Legend:

**BIND** = BIND request unit  
**BIND-RSP** = BIND response unit  
**ERD** = Encrypted random data  
**FMH-12** = Function Management Header 12  
**RD** = Random data

Obrázek 12. Toky pro ověření na úrovni relace

Protokol pro ověření úrovně relace je následující. Číslo v proceduře odpovídá číslům v [Obrázek 12 na stránce 103](#).

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 odevzvě BIND.
3. Když primární LU obdrží odevzvu 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 odevzvě 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 odevzvě BIND, a odešle šifrovaná data (ERD2) na sekundární LU v záhlaví správy funkcí 12 (FMH-12).

4. Když sekundární LU přijme FMH-12, vypočítá svou vlastní verzi šifrovaných dat z náhodných dat, která vygenerovala. Pak porovná jeho verzi s zašifrovanými daty, která přijala v FMH-12. Jsou-li tyto dvě



hodnoty stejné, je primární LU ověřena. Pokud se tyto dvě hodnoty neshodují, ukončí sekundární LU relaci.

V rozšířené verzi protokolu, která poskytuje lepší ochranu proti muži uprostřed napadení, vypočítá sekundární LU kód DES (Message Authentication Code) DES z RD1, RD2a plně kvalifikovaný název sekundární LU pomocí jeho kopie hesla LU-LU jako klíče. Sekundární LU odesílá MAC primární LU v rámci odezvy BIND místo ERD1.

Primární LU ověřuje sekundární LU pomocí výpočtu své vlastní verze MAC, která porovnává s MAC přijatou v odpovědi BIND. Primární logická jednotka potom vypočítá druhou adresu MAC z RD1 a RD2a místo ERD2odešle adresu MAC na sekundární logickou jednotku v FMH-12 .

Sekundární LU autentizuje primární LU tím, že si vyrovná svou vlastní verzi druhé MAC, která porovná s MAC přijatou v FMH-12.

Informace o tom, jak nakonfigurovat ověření úrovně relace, najdete v dokumentaci k subsystému SNA. Další obecné informace o ověřování na úrovni relace najdete v tématu *Systems Network Architecture LU 6.2 Reference: Peer Protocols, SC31-6808*.


#### *Ověření úrovně konverzace*

Když se lokální transakční program pokusí o přidělení konverzace s partnerským transakčním programem, odešle lokální LU operaci připojení k partnerské LU a požádá ji o připojení partnerského TP. Za určitých okolností může požadavek na připojení obsahovat informace o zabezpečení, které může partnerská LU použít k ověření lokálního transakčního protokolu. To se označuje jako *ověření na úrovni konverzace* nebo *ověření koncového uživatele*.


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

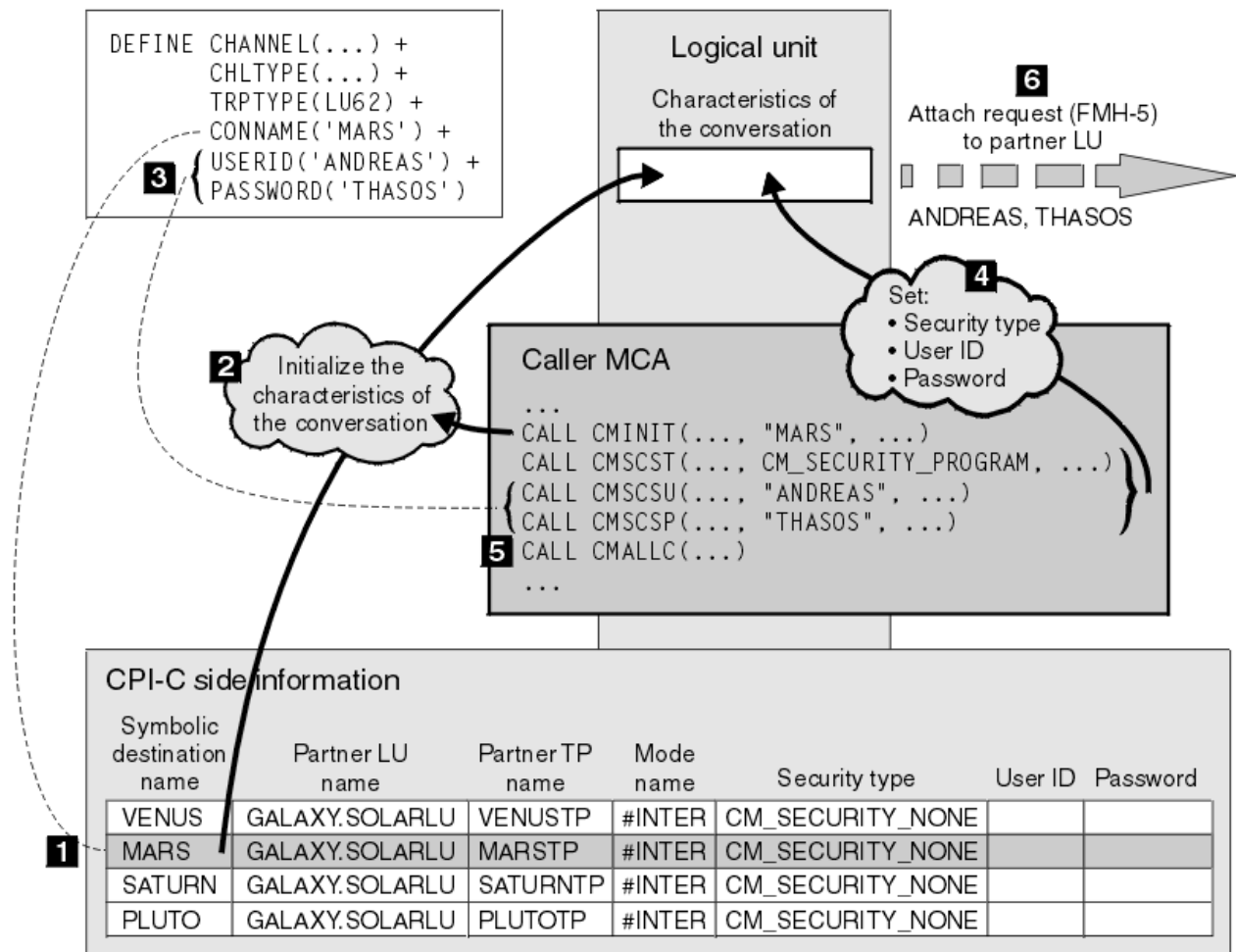
Další informace o ověřování na úrovni konverzace najdete v tématu *Systems Network Architecture LU 6.2 Reference: Peer Protocols, SC31-6808*. Informace specifické pro produkt z/OS naleznete v příručce *z/OS Planning: APPC/MVS Management, SA22-7599*.

Další informace o rozhraní CPI-C naleznete v příručce *Common Programming Interface Communications CPI-C Specification, SC31-6180*. Další informace o službách APPC/MVS CTP Callable Services naleznete v příručce *z/OS MVS Programming: Writing Transaction Programs for APPC/MVS, SA22-7621*.

Podpora pro ověření na úrovni konverzace v produktu IBM MQ v systémech  IBM i, Systémy SYSTÉM UNIXa Windows

V tomto tématu získáte přehled o tom, jak ověřování na úrovni konverzace funguje, na platformách jiných než z/OS.

Podpora autentizace na úrovni konverzace v IBM MQ pro  IBM i, IBM MQ na Systémy SYSTÉM UNIXa IBM MQ for Windows je ilustrována v Obrázek 13 na stránce 105. Čísla v diagramu odpovídají číslům v níže uvedeném popisu.



Obrázek 13. Podpora IBM MQ pro ověření na úrovni konverzace

U systémů IBM i, Systémy SYSTÉM UNIXa 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 přepíše jakékoli hodnoty získané dříve z informací o straně.

Volající MCA pak vydá volání CI-C CMALLC, aby přidělil konverzaci (5). V reakci na toto volání lokální jednotka LU odešle na partnerskou LU (6) požadavek na připojení (záhlaví správy funkcí 5 nebo FMH-5).

Pokud partnerská LU přijme ID uživatele a heslo, hodnoty USERID a PASSWORD jsou zahrnuty v požadavku na připojení. Pokud partnerská LU neakceptuje ID uživatele a heslo, hodnoty nebudou zahrnuty do požadavku na připojení. Lokální LU zjišťuje, zda partnerská LU přijme ID uživatele a heslo jako součást výměny informací, když se relace LU vytvoří pro vytvoření relace.

V novější verzi požadavku na připojení může nahradit heslo mezi jednotkami LU místo jednoznačných hesel. Náhradní heslo je kód DES (Message Authentication Code) DES nebo kód digest zprávy SHA-1 , vytvořený z hesla. Náhražky hesla lze použít pouze v případě, že je podporují obě LU.

Když partnerská LU přijme příchozí požadavek na připojení obsahující ID uživatele a heslo, může pro účely identifikace a ověření použít ID uživatele a heslo. S odkazem na seznamy přístupových práv může partnerská LU také určit, zda má ID uživatele oprávnění k přidělení konverzace a připojení agenta MCA.

Kromě toho může agent MCA být spuštěn pod ID uživatele zahrnutého v požadavku na připojení. V tomto případě se ID uživatele stane výchozím ID uživatele pro modul MCA odezvy a použije se pro kontroly oprávnění, když se agent MCA pokusí připojit ke správci front. Může být také použit pro kontroly oprávnění poté, co se agent MCA pokusí o přístup k prostředkům správce front.

Způsob, jakým lze ID uživatele a heslo v požadavku na připojení použít pro identifikaci, ověření a řízení přístupu, závisí na implementaci. Informace specifické pro váš subsystém SNA najdete v příslušné dokumentaci.

Není-li parametr USERID nastaven, volající agent MCA nezavolá funkce CMSCST, CMSCSU a CMSCSP. V tomto případě jsou informace o zabezpečení, které toky v požadavku na připojení tečou, určeny pouze tím, co je uvedeno v položce informací o straně a jaká partnerská LU bude přijímat.

#### *Ověřování na úrovni konverzace a IBM MQ for z/OS*

V tomto tématu získáte přehled o tom, jak funguje ověřování na úrovni konverzace, v systému z/OS.

V systému IBM MQ for z/OS MCA nevyužívá rozhraní CPI-C. Místo toho používají služby APPC/MVS TP Conversation Callable Services, což je implementace programu Advanced Program-to-Program Communication (APPC), která má některé funkce CPI-C. Když volající MCA alokuje konverzaci, je na volání uveden typ zabezpečení STEJNÝ. Vzhledem k tomu, že APPC/MVS LU podporuje trvalé ověření pouze pro příchozí konverzace, ne pro odchozí konverzace, existují dvě možnosti:

- Věřil-li partnerská LU APPC/MVS LU a přijme již ověřené ID uživatele, LU APPC/MVS odešle požadavek na připojení obsahující:
  - ID uživatele adresního prostoru inicializátoru kanálu
  - Název profilu zabezpečení, který, je-li použit RACF , je název aktuální skupiny připojení ID uživatele adresního prostoru iniciátoru kanálu
  - Již ověřený indikátor
- Pokud partnerská LU nedůvěřuje LU APPC/MVS a neakceptuje již ověřené ID uživatele, LU APPC/MVS odešle požadavek na připojení neobsahující žádné informace o zabezpečení.

V systému IBM MQ for z/OS nelze parametry USERID a PASSWORD u příkazu DEFINE CHANNEL použít pro kanál zpráv a jsou platné pouze na konci připojení klienta kanálu MQI. Proto požadavek na připojení z APPC/MVS LU nikdy neobsahuje hodnoty zadané těmito parametry.

## Zabezpečení klastrů správců front

Ačkoli mohou být klastry správců front vhodné k použití, je třeba věnovat zvláštní pozornost jejich zabezpečení.

*Klastr správců front* je síť správců front, kteří jsou nějakým způsobem logicky přidruženi. Správce front, který je členem klastru, se nazývá *správce front klastru*.

Frontu, která patří ke správci front klastru, může být známá ostatním správcům front v klastru. Taková fronta se nazývá *fronta klastru*. Kterýkoli správce front v klastru může odesílat zprávy do front klastru, aniž by bylo nutné některou z následujících položek:

- Explicitní definice vzdálených front pro každou frontu klastru.
- Explicitně definované kanály pro a z každého vzdáleného správce front
- Samostatná přenosová fronta pro každý odchozí kanál

Můžete vytvořit klastr, v němž jsou dva nebo více správců front klony. To znamená, že mají instance stejných lokálních front, včetně všech lokálních front deklarovaných jako fronty klastru, a mohou podporovat instance stejných serverových aplikací.

Odešle-li aplikace připojená ke správci front klastru zprávu do fronty klastru, která má instanci v každém z klonovaných správců front, produkt IBM MQ se rozhodne, kterému správci front má odeslat. Když mnoho aplikací odesílá zprávy do fronty klastru, IBM MQ vyrovnává pracovní zátěž mezi všemi správci front, kteří mají instanci fronty. Dojde-li k selhání jednoho ze systémů, které jsou hostiteli klonovaného správce front, bude produkt IBM MQ i nadále vyrovnávat pracovní zátěž mezi zbývajícími správci front, dokud nebude restartován systém, který selhal.

Používáte-li klastry správců front, je třeba zvážit následující otázky zabezpečení:

- Povolení odesílání zpráv do správce front pouze vybraným správcům front
- Povolení odesílání zpráv do fronty ve správci front pouze vybraným uživatelům vzdáleného správce front
- Povolení aplikací připojených k vašemu správci front pro odesílání zpráv pouze do vybraných vzdálených front


Tyto úvahy jsou relevantní i v případě, že nepoužíváte klastry, ale stávají se důležitějšími, pokud používáte klastry.

Pokud může aplikace odesílat zprávy do jedné fronty klastru, může odesílat zprávy do kterékoli jiné fronty klastru bez potřeby dalších definic vzdálených front, přenosových front nebo kanálů. Proto je důležité zvážit, zda je třeba omezit přístup ke frontám klastru ve správci front, a omezit fronty klastru, do kterých mohou aplikace odesílat zprávy.

Existují některé další aspekty zabezpečení, které jsou relevantní pouze v případě, že používáte klastry správců front:

- Povolení k připojení ke klastru pouze vybraným správcům front
- Vynucení opuštění klastru nechtěným správcům front

Další informace o všech těchto aspektech naleznete v tématu [Uchování zabezpečených klastrů](#).

 Informace o aspektech specifických pro produkt IBM MQ for z/OS naleznete v tématu [“Zabezpečení klastrů správců front v systému z/OS”](#) na stránce 246.

### Související úlohy

[“Zabránění příjmu zpráv správcem front”](#) na stránce 408

Můžete zabránit správci front klastru, aby přijímal zprávy, které nemá oprávnění přijímat, pomocí ukončovacích programů.

## Zabezpečení pro publikování/odběr produktu IBM MQ

Používáte-li produkt IBM MQ Publish/Subscribe, je třeba zvážit další aspekty zabezpečení.

V systému publikování/odběr existují dva typy aplikací: vydavatel a odběratel. *Vydavatelé* poskytují informace ve formě zpráv produktu IBM MQ . Když vydavatel publikuje zprávu, určuje *téma*, které identifikuje předmět informací uvnitř zprávy.

*Odběratelé* jsou spotřebiteli informací, které jsou publikovány. Odběratel určuje témata, která se zajímají o přihlášení k odběru.

*Správce front* je aplikace dodávaná s produktem IBM MQ Publish/Subscribe. Obdrží publikované zprávy od vydavatelů a požadavků na odběr od odběratelů a směřuje publikované zprávy na odběratele. Odběratel je odeslán pouze na ta témata, k jejichž odběru se přihlásili.

Další informace naleznete v tématu [Zabezpečení publikování a odběru](#).

## Zabezpečení výběrového vysílání

Tyto informace vám pomohou pochopit, proč mohou být procesy zabezpečení potřebné pro výběrové vysílání produktu IBM MQ .

Výběrové vysílání produktu IBM MQ nemá vestavěné zabezpečení. Kontroly zabezpečení se zpracovávají ve správci front v době MQOPEN a nastavení pole MQMD je obsluhováno klientem. Některé aplikace v síti nemusí být aplikace IBM MQ (například aplikace LLM, viz [Multicast Interoperability with IBM MQ Low Latency Messaging](#) pro více informací), proto byste mohli potřebovat implementovat vaše vlastní procedury zabezpečení, protože přijímající aplikace nemohou být některými z polí kontextu platnosti.

Je třeba zvážit tři procesy zabezpečení:

### Řízení přístupu

Řízení přístupu v produktu IBM MQ je založeno na ID uživatelů. Další informace o tomto tématu viz [“Řízení přístupu pro klienty” na stránce 83](#).

### 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 [“Koncepte šifrování” na stránce 7](#).

## Brány firewall a přímý průchod na Internet

Za normálních okolností byste měli používat ochrannou bariéru (firewall), abyste zabránili přístupu k nepřátelským adresám IP, například při útoku typu DoS (Denial of Service). Možná však budete muset dočasně blokovat adresy IP v rámci IBM MQ, možná i když počkáte na administrátora zabezpečení, aby aktualizoval pravidla brány firewall.

Chcete-li blokovat jednu nebo více adres IP, vytvořte záznam ověřování kanálu typu BLOCKADDR nebo ADDRESSMAP. Více informací naleznete v části [“Blokování určitých adres IP”](#) na stránce 362.

## Zabezpečení pro IBM MQ internet pass-thru

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

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

IBM MQ Internetový pass-thru umožňuje dvěma správcům front vyměňovat si zprávy nebo klientskou aplikaci IBM MQ pro připojení ke správci front bez nutnosti přímého připojení TCP/IP. To je užitečné, pokud brána firewall zakazuje přímé připojení TCP/IP mezi dvěma systémy. Proběhne průchod protokolu kanálu produktu IBM MQ a z brány firewall je jednodušší a lépe spravovatelný tunelováním toků uvnitř HTTP nebo serverem jako proxy. Pomocí TLS (Transport Layer Security) lze také používat k šifrování a dešifrování zpráv, které jsou odesílány přes Internet.

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

- Pokud se IPT chová jako server TLS a IBM MQ se připojuje jako klient TLS, musí CipherSpec používaná produktem IBM MQ odpovídat sadě CipherSuite, která je povolena v příslušném klíčovém kruhu IPT.
- Pokud IPT vystupuje jako klient TLS a připojuje se k serveru IBM MQ TLS, musí IPT CipherSuite odpovídat sadě CipherSpec definované v přijímajícím kanálu produktu IBM MQ.

Pokud migrujete z IPT na integrovanou podporu TLS IBM MQ, přeneste digitální certifikáty z IPT pomocí `mqiPTKeyman` nebo `mqiPTKeycmd`.

Další informace naleznete v dokumentu [IBM MQ Internet Pass-Thru \(SupportPac MS81\)](#).

## Kontrolní seznam implementace zabezpečení produktu IBM MQ for z/OS

Toto téma poskytuje proceduru step-by-step, kterou můžete použít k práci a definování implementace zabezpečení pro každého správce front produktu IBM MQ.

RACF poskytuje definice pro třídy zabezpečení IBM MQ v dodané statické tabulce deskriptoru třídy (CDT). Při práci s kontrolním seznamem můžete určit, které z těchto tříd vaše nastavení vyžaduje. Musíte se ujistit, že jsou aktivovány, jak je popsáno v tématu [“Třídy zabezpečení produktu RACF”](#) na stránce 171.

Podrobnosti naleznete v dalších částech, konkrétně [“Profily používané k řízení přístupu k prostředkům produktu IBM MQ”](#) na stránce 181.

Pokud vyžadujete kontrolu zabezpečení, postupujte podle tohoto kontrolního seznamu a implementujte jej:

1. Aktivujte třídu MQADMIN produktu RACF (velké profily) nebo MXADMIN (se smíšenými profily případů).
  - Chcete zabezpečení na úrovni skupiny sdílení front, na úrovni správce front, nebo kombinaci obou těchto voleb?  
Viz téma [“Profily pro řízení zabezpečení na úrovni skupiny sdílení front nebo správce front”](#) na stránce 176.
2. Potřebujete zabezpečení připojení?

- **Ano:** Aktivujte třídu MQCONN. Definujte příslušné profily připojení na úrovni správce front nebo na úrovni skupiny sdílení front ve třídě MQCONN. Poté povolte příslušným uživatelům nebo skupinám přístup k těmto profilům.
- Poznámka:** Přístup k odpovídajícímu profilu připojení mohou mít pouze uživatelé požadavku rozhraní API MQCONN nebo CICS nebo ID uživatelů adresního prostoru IMS .
- **Ne:** Definujte hlq.NO.CONNECT.CHECKS profil buď na úrovni správce front, nebo na úrovni skupiny sdílení front ve třídě MQADMIN nebo MXADMIN.
3. Potřebujete kontrolu zabezpečení u příkazů?
- **Ano:** Aktivujte třídu MQCMDS. Definujte příslušné profily příkazů buď na úrovni správce front, nebo na úrovni skupiny sdílení front ve třídě MQCMDS. Poté povolte příslušným uživatelům nebo skupinám přístup k těmto profilům.
- Používáte-li skupinu sdílení front, může být nutné zahrnout ID uživatelů používaná samotným správcem front a inicializačním inicializačním kanálem. Viz [“Nastavení zabezpečení prostředků produktu IBM MQ for z/OS”](#) na stránce 238.
- **Ne:** Definujte hlq.NO.CMD.CHECKS profil pro požadovaného správce front nebo skupinu sdílení front ve třídě MQADMIN nebo MXADMIN.
4. Potřebujete zabezpečení na prostředcích použitých v příkazech?
- **Ano:** Ujistěte se, že je třída MQADMIN nebo MXADMIN aktivní. Definujte příslušné profily pro ochranu prostředků u příkazů na úrovni správce front nebo na úrovni skupiny sdílení front ve třídě MQADMIN nebo MXADMIN. Poté povolte příslušným uživatelům nebo skupinám přístup k těmto profilům. Nastavte parametr CMDUSER v souboru CSQ6SYSP na výchozí ID uživatele, které má být použito pro kontroly zabezpečení příkazů.
- Používáte-li skupinu sdílení front, může být nutné zahrnout ID uživatelů používaná samotným správcem front a inicializačním inicializačním kanálem. Viz [“Nastavení zabezpečení prostředků produktu IBM MQ for z/OS”](#) na stránce 238.
- **Ne:** Definujte hlq.NO.CMD.RESC.CHECKS profil pro požadovaného správce front nebo skupinu sdílení front ve třídě MQADMIN nebo MXADMIN.
5. Potřebujete zabezpečení fronty?
- **Ano:** Aktivujte třídu MQQUEUE nebo MXQUEUE. Definujte příslušné profily fronty pro požadovaného správce front nebo skupinu sdílení front ve třídě MQQUEUE nebo MXQUEUEclass. Poté povolte příslušným uživatelům nebo skupinám přístup k těmto profilům.
  - **Ne:** Definujte hlq.NO.QUEUE.CHECKS profil pro požadovaného správce front nebo skupinu sdílení front ve třídě MQADMIN nebo MXADMIN.
6. Potřebujete zabezpečení procesu?
- **Ano:** Aktivujte třídu MQPROC nebo MXPROC. Definujte příslušné profily procesu na úrovni správce front nebo skupiny sdílení front a povolte těmto profilům přístup k příslušným uživatelům nebo skupinám.
  - **Ne:** Definujte hlq.NO.PROCESS.CHECKS profil pro příslušného správce front nebo skupinu sdílení front ve třídě MQADMIN nebo MXADMIN.
7. Potřebujete zabezpečení seznamu názvů?
- **Ano:** Aktivace třídy MQNLIST nebo MXNLISTclass. Definujte příslušné profily seznamu názvů na úrovni správce front nebo na úrovni skupiny sdílení front v rámci třídy MQNLIST nebo MXNLIST. Poté povolte příslušným uživatelům nebo skupinám přístup k těmto profilům.
  - **Ne:** Definujte hlq.NO.NLIST.CHECKS profil pro požadovaného správce front nebo skupinu sdílení front ve třídě MQADMIN nebo MXADMIN.
8. Potřebujete zabezpečení témat?
- **Ano:** Aktivujte třídu MXTOPIC. Definujte příslušné profily témat buď na úrovni správce front, nebo na úrovni skupiny sdílení front ve třídě MXTOPIC. Poté povolte příslušným uživatelům nebo skupinám přístup k těmto profilům.



- **Ne:** Definujte hlq.NO.TOPIC.CHECKS profil pro požadovaného správce front nebo skupinu sdílení front ve třídě MQADMIN nebo MXADMIN.
9. Je třeba, aby všichni uživatelé chránili použití voleb MQOPEN nebo MQPUT1 souvisejících s použitím kontextu?
- **Ano:** Ujistěte se, že je třída MQADMIN nebo MXADMIN aktivní. Definujte profily hlq.CONTEXT.queueaname na úrovni fronty, správce front nebo skupiny sdílení front ve třídě MQADMIN nebo MXADMIN. Poté povolte příslušným uživatelům nebo skupinám přístup k těmto profilům.
  - **Ne:** Definujte hlq.NO.CONTEXT.CHECKS profil pro požadovaného správce front nebo skupinu sdílení front ve třídě MQADMIN nebo MXADMIN.
10. Potřebujete chránit používání alternativních ID uživatelů?
- **Ano:** Ujistěte se, že je třída MQADMIN nebo MXADMIN aktivní. Definujte příslušnou položku hlq.ALTERNATE.USER. *alternateuserid* profilů pro požadovaného správce front nebo skupiny sdílení front a povolení přístupu požadovaných uživatelů nebo skupin k těmto profilům.
  - **Ne:** Definujte profil hlq.NO.ALTERNATE.USER.CHECKS pro požadovaného správce front nebo skupinu sdílení front ve třídě MQADMIN nebo MXADMIN.
11. Potřebujete přizpůsobit ID uživatelů, která ID uživatele mají být použita pro kontroly zabezpečení prostředků prostřednictvím RESLEVEL?
- **Ano:** Ujistěte se, že je třída MQADMIN nebo MXADMIN aktivní. Definujte profil hlq.RESLEVEL buď na úrovni správce front, nebo na úrovni skupiny sdílení front ve třídě MQADMIN nebo MXADMIN. Poté povolte požadovaný přístup uživatelů nebo skupin k profilu.
  - **Ne:** Ujistěte se, že ve třídě MQADMIN nebo MXADMIN neexistují žádné generické profily, které lze použít na hlq.RESLEVEL. Definujte profil hlq.RESLEVEL pro požadovaného správce front nebo skupinu sdílení front a ujistěte se, že k němu nemají přístup žádní uživatelé nebo skupiny.
12. Potřebujete 'timeout' nepoužité ID uživatele z IBM MQ ?
- **Ano:** Určete hodnoty časového limitu, které byste chtěli použít, a vydejte příkaz MQSC ALTER SECURITY, abyste změnili parametry TIMEOUT a INTERVAL.
  - **Ne:** Vydejte příkaz MQSC ALTER SECURITY, abyste nastavili hodnotu INTERVAL na nulu.
- Poznámka:** Aktualizujte vstupní datovou sadu inicializace CSQINP1 používanou vašim podsystémem tak, aby byl příkaz MQSC ALTER SECURITY vydán automaticky při spuštění správce front.
13. Používáte distribuované fronty?
- **Ano:** Použít záznamy ověření kanálu. Další informace viz [“Záznamy ověření kanálu”](#) na stránce 48.
  - Můžete také určit příslušnou hodnotu atributu MCAUSER pro každý kanál nebo poskytnout vhodné uživatelské procedury zabezpečení kanálu.
14. Chcete použít SSL (Secure Sockets Layer)?
- **Ano:** Chcete-li určit, že každý uživatel, který prezentuje osobní certifikát SSL/TLS obsahující zadané DN, má používat specifický MCAUSER, nastavit záznam ověřování kanálu typu SSLPEERMAP. Můžete zadat jeden rozlišující název nebo vzorec zahrnující zástupné znaky.
  - Naplánujte infrastrukturu SSL. Nainstalujte funkci System SSL produktu z/OS. V produktu RACFnastavte své filtry názvů certifikátů (CNFs), pokud je používáte, a své digitální certifikáty. Nastavte svazek klíčů SSL. Ujistěte se, že atribut SSLKEYR správce front je neprázdný a ukazuje na váš svazek klíčů SSL. Také se ujistěte, že hodnota SSLTASKS je alespoň 2.
  - **Ne:** Ujistěte se, že SSLKEYR je prázdné, a SSLTASKS je nula.
- Další informace o SSL viz [“Protokoly zabezpečení SSL a TLS v produktu IBM MQ”](#) na stránce 22.
15. Používám klienty?
- **Ano:** Použít záznamy ověření kanálu.
  - Můžete také určit příslušnou hodnotu atributu MCAUSER pro každý kanál připojení serveru nebo v případě potřeby poskytnout vhodné uživatelské procedury zabezpečení kanálu.

16. Zkontrolujte nastavení přepínače.

Produkt IBM MQ generuje zprávy při spuštění správce front, které zobrazují vaše nastavení zabezpečení. Použijte tyto zprávy k určení, zda jsou vaše přepínače nastaveny správně.

17. Posíláte hesla od klientských aplikací?

- **Ano:** Ujistěte se, že je nainstalována funkce produktu z/OS a je spuštěna služba Integrated Cryptographic Service Facility (ICSF) pro nejlepší ochranu.
- **Ne:** Můžete ignorovat chybovou zprávu oznamující, že ICSF není spuštěno.

Další informace o programu ICSF najdete v tématu [“Použití programu ICSF \(Integrated Cryptographic Service Facility\)”](#) na stránce 246

## Nastavení zabezpečení

---

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

### Nastavení zabezpečení v systémech Windows, SYSTÉM UNIX a Linux

Aspekty zabezpečení specifické pro systémy Windows, SYSTÉM UNIX a Linux .

Správci front produktu IBM MQ přenášejí informace, které jsou potenciálně cenné, a proto je třeba pomocí systému oprávnění zajistit, aby neautorizovaní uživatelé nemohli přistupovat k vašim správcům front. Zvažte následující typy ovládacích prvků zabezpečení:

#### Kdo může spravovat produkt IBM MQ

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

#### Kdo může používat objekty produktu IBM MQ

Můžete definovat, kteří uživatelé (obvykle aplikace) mohou použít volání MQI a PCF příkazy k provedení následujících úloh:

- Kdo se může připojit ke správci front.
- Kdo může přistupovat k objektům (fronty, definice procesů, seznamy názvů, kanály, kanály připojení klienta, moduly listener, služby a objekty ověřovacích informací) a jaký typ přístupu k těmto objektům mají.
- Kdo má přístup k zprávám produktu IBM MQ .
- Kdo má přístup ke kontextovým informacím přidruženým ke zprávě.

#### Zabezpečení kanálu

Je třeba zajistit, aby kanály používané k odesílání zpráv na vzdálené systémy měly přístup k požadovaným prostředkům.

Pro udělování přístupu k knihovnám programů, knihovnám odkazů MQI a příkazům můžete použít standardní provozní prostředky. Avšak adresář obsahující fronty a další data správce front je pro produkt IBM MQsoukromý; nepoužívejte standardní příkazy operačního systému k udělení nebo zrušení autorizace k prostředkům MQI.

### Autorizování uživatelů pro vzdálené použití produktu IBM MQ

Potřebujete-li vytvořit a spustit správce front při vzdáleném připojení k produktu IBM MQ , musíte mít k dispozici uživatelský přístup Vytvořit globální objekty .

#### Informace o této úloze

**Poznámka:** Administrátoři mají při výchozím nastavení přístup uživatele Vytvořit globální objekty , takže pokud jste administrátorem, můžete vytvářet a spouštět správce front při vzdáleném připojení, aniž by došlo ke změně vašich uživatelských práv.

Pokud se připojujete k počítači s produktem Windows pomocí služeb Terminal Services nebo Remote Desktop Connection a máte problémy s vytvářením, spouštěním nebo odstraněním správce front, může to být způsobeno tím, že nemáte přístup uživatele Vytvořit globální objekty.

Uživatelský přístup Vytvořit globální objekty omezuje uživatele, kteří mají oprávnění k vytváření objektů v globálním oboru názvů. Má-li aplikace vytvořit globální objekt, musí být buď spuštěn v globálním oboru názvů, nebo uživatel, pod kterým je spuštěna aplikace, musí mít na něj použitý uživatelský přístup Vytvořit globální objekty.

Když se připojujete vzdáleně k počítači se systémem Windows pomocí služeb Terminal Services nebo Remote Desktop Connection, aplikace běží ve svém vlastním lokálním oboru názvů. If you attempt to create or delete a queue manager using MQ Explorer or the **crtmqm** or **dltmqm** command, or to start a queue manager using the **strmqm** command, it results in an authorization failure. Tím se vytvoří FDC IBM MQ s ID sondy XY132002.

Spuštění správce front pomocí příkazu MQ Explorernebo použití příkazu **amqmdain qmgr start** funguje správně, protože tyto příkazy přímo nespouští správce front. Místo toho příkazy odešlou požadavek na spuštění správce front do samostatného procesu spuštěného v globálním oboru názvů.

Pokud různé metody administrace IBM MQ nefungují při použití terminálových služeb, pokuste se nastavit uživatele Vytvořit globální objekty správně.

## Postup

1. Otevřete panel Administrativní nástroje:

### **Windows Server 2008 a Windows Server 2012**

Tento panel otevřete pomocí nabídky **Ovládací panely > Systém a údržba > Administrativní nástroje**.

### **Windows 8.1**

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

2. Poklepejte na položku **Lokální zásada zabezpečení**.
3. Rozbalte **Lokální zásady**.
4. Klepněte na volbu **Přiřazení práv uživatele**.
5. Přidejte nového uživatele nebo skupinu do zásady Vytvořit globální objekty.

## 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 Server 2008 a Windows Server 2012**

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

### **Windows 7 a Windows 8.1**

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 uživatele ve skupině v systému Windows***

Zobrazit členy skupiny pomocí ovládacího panelu.

## Postup

1. Otevřete ovládací panel
2. Poklepejte na **Administrativní nástroje**.  
Otevře se panel Administrativní nástroje.
3. Dvakrát klepněte na volbu **Správa počítače**.  
Otevře se panel Správa počítačů.
4. V panelu Správa počítačů rozbalte **Lokální uživatelé a skupiny**.
5. Vyberte **Skupiny**.
6. Poklepejte na skupinu. Zobrazí se panel vlastností skupiny.  
Zobrazí se panel vlastností skupiny.

## Výsledky

Zobrazí se členové skupiny.

## 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 za předpokladu, že nepoužíváte NIS nebo NIS +, použijte správce správy systému (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 uživatele 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 odebrání 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 `groupaa` stane se členem `groupb`, použijte následující příkaz: `usermod -G groupa,groupb user-name`, kde *jméno-uživatele* je jméno uživatele.

### Zobrazení uživatele 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`, použijte se následující příkaz: `usermod -G groupa,groupb user-name`, kde *user-name* je jméno uživatele.

## Vytvoření a správa skupin v systému Linux

V systému Linux za 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 `groupaa` 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 +setallatd. Tyto konstanty jsou definovány v souboru záhlaví cmqzc.h dodaném 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 10 na stránce 120, Tabulka 11 na stránce 120, Tabulka 12 na stránce 121 a Tabulka 13 na stránce 122 sumarizují oprávnění potřebná pro každé volání. V tabulkách *Nepoužitelné* znamená, že kontrola autorizace není pro tuto operaci relevantní; *Bez kontroly* znamená, že se neprovádí žádná kontrola autorizace.

**Poznámka:** V těchto tabulkách nenajdete žádné zmínky o kanálech názvů, kanálech, kanálech připojení klienta, modulech listener, službách nebo objektech ověřovacích informací. Důvodem je to, že se na tyto objekty nevztahují žádná oprávnění, s výjimkou MQOO\_INQUIRE, pro které platí stejná oprávnění jako pro ostatní objekty.

Speciální autorizace MQZAO\_ALL\_MQI obsahuje všechny autorizace v tabulkách, které jsou relevantní pro daný typ objektu, s výjimkou MQZADELETE DELETE a MQZAO\_DISPLAY, které jsou klasifikovány jako autorizace pro administraci.

Chcete-li upravit kteroukoli z voleb kontextu zprávy, musíte mít příslušná oprávnění k vydávání volání. Chcete-li například použít funkci MQOO\_SET\_IDENTITY\_CONTEXT nebo MQPMO\_SET\_IDENTITY\_CONTEXT, musíte mít oprávnění +setid.

<i>Tabulka 10. Autorizace zabezpečení potřebná pro volání MQCONN</i>			
<b>Je vyžadována autorizace pro:</b>	<b>Objekt fronty ( "1" na stránce 122 )</b>	<b>Objekt procesu</b>	<b>Objekt správce front</b>
<b>MQCONN</b>	Nelze použít	Nelze použít	MQZAO_PŘIPOJENÍ

<i>Tabulka 11. Autorizace zabezpečení potřebná pro volání MQOPEN</i>			
<b>Je vyžadována autorizace pro:</b>	<b>Objekt fronty ( "1" na stránce 122 )</b>	<b>Objekt procesu</b>	<b>Objekt správce front</b>
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 122 )	MQZAO_VSTUP	Nelze použít	Nelze použít
MQOO_OUTPUT (normální fronta) ( "3" na stránce 122 )	MQZAO_VÝSTUP	Nelze použít	Nelze použít

<i>Tabulka 11. Autorizace zabezpečení potřebná pro volání MQOPEN (pokračování)</i>			
<b>Je vyžadována autorizace pro:</b>	<b>Objekt fronty ( “1” na stránce 122 )</b>	<b>Objekt procesu</b>	<b>Objekt správce front</b>
MQOO_PASS_IDENTITY_CONTEXT ( “4” na stránce 122 )	MQZAO_PASS_IDENTITY_CONTEXT	Nelze použít	Žádná kontrola
MQOO_PASS_ALL_CONTEXT ( “4” na stránce 122, “5” na stránce 122 )	MQZAO_PASS_ALL_CONTEXT	Nelze použít	Žádná kontrola
MQOO_SET_IDENTITY_CONTEXT ( “4” na stránce 122, “5” na stránce 122 )	MQZAO_SET_IDENTITY_CONTEXT	Nelze použít	MQZA_SET_IDENTITY_CONTEXT ( “6” na stránce 122 )
MQOO_SET_ALL_CONTEXT ( “4” na stránce 122, “7” na stránce 122 )	MQZAO_SET_ALL_CONTEXT	Nelze použít	MQZA_SET_ALL_CONTEXT ( “6” na stránce 122 )
MQOO_OUTPUT (Přenosová fronta) ( “8” na stránce 122 )	MQZAO_SET_ALL_CONTEXT	Nelze použít	MQZA_SET_ALL_CONTEXT ( “6” na stránce 122 )
MQOOK_SADA	MQZAO_SADA	Nelze použít	Žádná kontrola
MQO_ALTERNATE_USER_AUTHORITY	( “9” na stránce 122 )	( “9” na stránce 122 )	MQZAO_ALTERNATE_USER_AUTHORITY ( “9” na stránce 122, “10” na stránce 122 )

<i>Tabulka 12. Autorizace zabezpečení potřebná pro volání MQPUT1</i>			
<b>Je vyžadována autorizace pro:</b>	<b>Objekt fronty ( “1” na stránce 122 )</b>	<b>Objekt procesu</b>	<b>Objekt správce front</b>
KONTEXT MQPMO_PASS_IDENTITY_CONTEXT	MQZA_PASS_IDENTITY_CONTEXT ( “11” na stránce 122 )	Nelze použít	Žádná kontrola
MQPMO_PASS_ALL_CONTEXT	MQZA_PASS_ALL_CONTEXT ( “11” na stránce 122 )	Nelze použít	Žádná kontrola
KONTEXT MQPMO_SET_IDENTITY_CONTEXT	MQZA_SET_IDENTITY_CONTEXT ( “11” na stránce 122 )	Nelze použít	MQZA_SET_IDENTITY_CONTEXT ( “6” na stránce 122 )
MQPMO_SET_ALL_CONTEXT	MQZA_SET_ALL_CONTEXT ( “11” na stránce 122 )	Nelze použít	MQZA_SET_ALL_CONTEXT ( “6” na stránce 122 )
(Přenosová fronta) ( “8” na stránce 122 )	MQZAO_SET_ALL_CONTEXT	Nelze použít	MQZA_SET_ALL_CONTEXT ( “6” na stránce 122 )
MQPMO_ALTERNATE_USER_AUTHORITY	( “12” na stránce 122 )	Nelze použít	MQZAO_ALTERNATE_USER_AUTHORITY ( “10” na stránce 122 )

Tabulka 13. Autorizace zabezpečení potřebná pro volání MQCLOSE

Je vyžadována autorizace pro:	Objekt fronty ( "1" na stránce 122 )	Objekt procesu	Objekt správce front
MQCO_DELETE	MQZAO_DELETE ( "13" na stránce 122 )	Nelze použít	Nelze použít
VYPRÁZDNIT ODSTRANĚNÍ MQCO_DELETE	MQZAO_DELETE ( "13" na stránce 122 )	Nelze použít	Nelze použít

#### Poznámky k tabulkám:

- 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.
- Musí být zadán také parametr MQOO\_INPUT\_\*. To platí pro lokální frontu, model nebo alias frontu.
- Tato kontrola se provádí pro všechny výstupní případy s výjimkou přenosových front (viz poznámka "8" na stránce 122).
- Musí být zadán také parametr MQOO\_OUTPUT.
- Tuto volbu má také implikovaná hodnota MQO\_P\_PASS\_IDENTITY\_CONTEXT.
- Toto oprávnění je povinné jak pro objekt správce front, tak pro konkrétní frontu.
- Tato volba předpokládá také MQOO\_PASS\_IDENTITY\_CONTEXT, MQOO\_PASS\_ALL\_CONTEXT a MQOO\_SET\_IDENTITY\_CONTEXT.
- 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).
- 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.
- Toto oprávnění umožňuje zadat jakékoli *AlternateUserId*.
- Kontrola MQZAO\_OUTPUT se provádí také tehdy, pokud fronta nemá atribut fronty *Usage* MQUS\_TRANSMISSION.
- 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.
- 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**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Fronta	ZMĚNA MQZAO_CHANGE
Téma	ZMĚNA MQZAO_CHANGE
Proces	ZMĚNA MQZAO_CHANGE
Správce front	ZMĚNA MQZAO_CHANGE
Seznam názvů	ZMĚNA MQZAO_CHANGE
Ověřovací informace	ZMĚNA MQZAO_CHANGE
Kanál	ZMĚNA MQZAO_CHANGE
Kanál připojení klienta	ZMĚNA MQZAO_CHANGE
Modul listener	ZMĚNA MQZAO_CHANGE
Služba	ZMĚNA MQZAO_CHANGE
Informace o komunikaci	ZMĚNA MQZAO_CHANGE

#### **CLEAR objekt**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
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 127 )**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Fronta	MQZAO_CREATE ( "2" na stránce 127 )
Téma	MQZAO_CREATE ( "2" na stránce 127 )
Proces	MQZAO_CREATE ( "2" na stránce 127 )
Správce front	Nelze použít

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Seznam názvů	MQZAO_CREATE ( <b>"2"</b> na stránce 127 )
Ověřovací informace	MQZAO_CREATE ( <b>"2"</b> na stránce 127 )
Kanál	MQZAO_CREATE ( <b>"2"</b> na stránce 127 )
Kanál připojení klienta	MQZAO_CREATE ( <b>"2"</b> na stránce 127 )
Modul listener	MQZAO_CREATE ( <b>"2"</b> na stránce 127 )
Služba	MQZAO_CREATE ( <b>"2"</b> na stránce 127 )
Informace o komunikaci	MQZAO_CREATE ( <b>"2"</b> na stránce 127 )

**DEFINE objekt REPLACE ( **"1"** na stránce 127, **"3"** na stránce 127 )**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
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**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
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**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Fronta	MQZAO_ZOBRAZENÍ
Téma	MQZAO_ZOBRAZENÍ
Proces	MQZAO_ZOBRAZENÍ
Správce front	MQZAO_ZOBRAZENÍ
Seznam názvů	MQZAO_ZOBRAZENÍ
Ověřovací informace	MQZAO_ZOBRAZENÍ
Kanál	MQZAO_ZOBRAZENÍ
Kanál připojení klienta	MQZAO_ZOBRAZENÍ
Modul listener	MQZAO_ZOBRAZENÍ
Služba	MQZAO_ZOBRAZENÍ
Informace o komunikaci	MQZAO_ZOBRAZENÍ

**START objekt**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
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**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Fronta	Nelze použít
Téma	Nelze použít
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít
Ověřovací informace	Nelze použít
Kanál	MQZAO_CONTROL

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

### Příkazy kanálu

Příkaz	Objekt	Je vyžadována autorizace
Odeslat signál Ping pro kanál	Kanál	MQZAO_CONTROL
Resetovat kanál	Kanál	MQZAO_CONTROL_EXTENDED
Vyřešit kanál	Kanál	MQZAO_CONTROL_EXTENDED

### Příkazy odběrů

Příkaz	Objekt	Je vyžadována autorizace
ZMĚNIT DÍLČÍ	Téma	MQZAO_CONTROL
DEFINE SUB	Téma	MQZAO_CONTROL
ODSTRANIT DÍLČÍ	Téma	MQZAO_CONTROL
ZOBRAZIT POD	Téma	MQZAO_ZOBRAZENÍ

### Příkazy pro zabezpečení

Příkaz	Objekt	Je vyžadována autorizace
SET AUTHREC	Správce front	ZMĚNA MQZAO_CHANGE
ODSTRANIT AUTHREC	Správce front	ZMĚNA MQZAO_CHANGE
ZOBRAZIT AUTHREC	Správce front	MQZAO_ZOBRAZENÍ
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

Příkaz	Objekt	Je vyžadována autorizace
ZOBRAZIT STAV SBSTATUS	Správce front	MQZAO_ZOBRAZENÍ
ZOBRAZIT STAV SVSTATUS	Správce front	MQZAO_ZOBRAZENÍ
ZOBRAZIT STAV TPSTATUS	Správce front	MQZAO_ZOBRAZENÍ

### Příkazy klastru

Příkaz	Objekt	Je vyžadována autorizace
ZOBRAZIT CLUQMGR	Správce front	MQZAO_ZOBRAZENÍ
Aktualizovat klastr	Vyžadováno členství ve skupině 'mqm'	
Reset klastru	Vyžadováno členství ve skupině 'mqm'	
SUSPEND QMgr	Vyžadováno členství ve skupině 'mqm'	
OBNOVIT SPRÁVCE FRONT	Vyžadováno členství ve skupině 'mqm'	

### Další administrativní příkazy

Příkaz	Objekt	Je vyžadována autorizace
ODESLÁNÍ PŘÍKAZU PING	Správce front	MQZAO_ZOBRAZENÍ
AKTUALIZOVAT SPRÁVCE FRONT	Správce front	ZMĚNA MQZAO_CHANGE
RESETOVAT QMGR	Správce front	ZMĚNA MQZAO_CHANGE
ZOBRAZIT PŘIPOJENÍ	Správce front	MQZAO_ZOBRAZENÍ
ZASTAVIT PŘIPOJENÍ	Správce front	ZMĚNA MQZAO_CHANGE

### Poznámka:

1. Pro příkazy DEFINE je pro objekt LIKE také zapotřebí oprávnění MQZAO\_DISPLAY, je-li zadán, nebo na příslušném SYSTEM.DEFAULT.xxx, je-li LIKE vynechán.
2. Oprávnění CREATE MQZAO\_CREATE není specifické pro konkrétní objekt nebo typ objektu. Oprávnění k vytvoření je uděleno pro všechny objekty pro určitého správce front, 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**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
<a href="#">Fronta</a>	ZMĚNA MQZAO_CHANGE
<a href="#">Téma</a>	ZMĚNA MQZAO_CHANGE
<a href="#">Proces</a>	ZMĚNA MQZAO_CHANGE
<a href="#">správce front</a>	ZMĚNA MQZAO_CHANGE
<a href="#">Seznam názvů</a>	ZMĚNA MQZAO_CHANGE
<a href="#">Ověřovací informace</a>	ZMĚNA MQZAO_CHANGE
<a href="#">Kanál</a>	ZMĚNA MQZAO_CHANGE
<a href="#">Kanál připojení klienta</a>	ZMĚNA MQZAO_CHANGE
<a href="#">Modul listener</a>	ZMĚNA MQZAO_CHANGE
<a href="#">Služba</a>	ZMĚNA MQZAO_CHANGE
<a href="#">Informace o komunikaci</a>	ZMĚNA MQZAO_CHANGE

**Vymazat objekt**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
<a href="#">Fronta</a>	MQZAO_CLEAR
<a href="#">Téma</a>	MQZAO_CLEAR
<a href="#">Proces</a>	Nelze použít
<a href="#">Správce front</a>	Nelze použít
<a href="#">Seznam názvů</a>	Nelze použít
<a href="#">Ověřovací informace</a>	Nelze použít
<a href="#">Kanál</a>	Nelze použít
<a href="#">Kanál připojení klienta</a>	Nelze použít
<a href="#">Modul listener</a>	Nelze použít
<a href="#">Služba</a>	Nelze použít
<a href="#">Informace o komunikaci</a>	Nelze použít

**Kopírování objekt (bez náhrady) ( 1 )**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
<a href="#">Fronta</a>	MQZAO_CREATE ( <b>2</b> )
<a href="#">Téma</a>	MQZAO_CREATE ( <b>2</b> )
<a href="#">Proces</a>	MQZAO_CREATE ( <b>2</b> )
<a href="#">Správce front</a>	Nelze použít
<a href="#">Seznam názvů</a>	MQZAO_CREATE ( <b>2</b> )
<a href="#">Ověřovací informace</a>	MQZAO_CREATE ( <b>2</b> )
<a href="#">Kanál</a>	MQZAO_CREATE ( <b>2</b> )

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
<u>Kanál připojení klienta</u>	MQZAO_CREATE ( <b>2</b> )
<u>Modul listener</u>	MQZAO_CREATE ( <b>2</b> )
<u>Služba</u>	MQZAO_CREATE ( <b>2</b> )
<u>Informace o komunikaci</u>	MQZAO_CREATE ( " <b>2</b> " na stránce 133 )

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

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
<u>Fronta</u>	ZMĚNA MQZAO_CHANGE
<u>Téma</u>	ZMĚNA MQZAO_CHANGE
<u>Proces</u>	ZMĚNA MQZAO_CHANGE
<u>Správce front</u>	Nelze použít
<u>Seznam názvů</u>	ZMĚNA MQZAO_CHANGE
<u>Ověřovací informace</u>	ZMĚNA MQZAO_CHANGE
<u>Kanál</u>	ZMĚNA MQZAO_CHANGE
<u>Kanál připojení klienta</u>	ZMĚNA MQZAO_CHANGE
<u>Modul listener</u>	ZMĚNA MQZAO_CHANGE
<u>Služba</u>	ZMĚNA MQZAO_CHANGE
<u>Informace o komunikaci</u>	ZMĚNA MQZAO_CHANGE

**Vytvořit objekt (bez náhrady) ( 3 )**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
<u>Fronta</u>	MQZAO_CREATE ( <b>2</b> )
<u>Téma</u>	MQZAO_CREATE ( <b>2</b> )
<u>Proces</u>	MQZAO_CREATE ( <b>2</b> )
<u>Správce front</u>	Nelze použít
<u>Seznam názvů</u>	MQZAO_CREATE ( <b>2</b> )
<u>Ověřovací informace</u>	MQZAO_CREATE ( <b>2</b> )
<u>Kanál</u>	MQZAO_CREATE ( <b>2</b> )
<u>Kanál připojení klienta</u>	MQZAO_CREATE ( <b>2</b> )
<u>Modul listener</u>	MQZAO_CREATE ( <b>2</b> )
<u>Služba</u>	MQZAO_CREATE ( <b>2</b> )
<u>Informace o komunikaci</u>	MQZAO_CREATE ( <b>2</b> )

**Vytvořte objekt (s nahrazením) ( 3, 4 )**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
<u>Fronta</u>	ZMĚNA MQZAO_CHANGE
<u>Téma</u>	ZMĚNA MQZAO_CHANGE

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
<u>Proces</u>	ZMĚNA MQZAO_CHANGE
Správce front	Nelze použít
<u>Seznam názvů</u>	ZMĚNA MQZAO_CHANGE
<u>Ověřovací informace</u>	ZMĚNA MQZAO_CHANGE
<u>Kanál</u>	ZMĚNA MQZAO_CHANGE
<u>Kanál připojení klienta</u>	ZMĚNA MQZAO_CHANGE
<u>Modul listener</u>	ZMĚNA MQZAO_CHANGE
<u>Služba</u>	ZMĚNA MQZAO_CHANGE
<u>Informace o komunikaci</u>	ZMĚNA MQZAO_CHANGE

### **Odstranit objekt**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
<u>Fronta</u>	MQZAO_DELETE
<u>Téma</u>	MQZAO_DELETE
<u>Proces</u>	MQZAO_DELETE
Správce front	Nelze použít
<u>Seznam názvů</u>	MQZAO_DELETE
<u>Ověřovací informace</u>	MQZAO_DELETE
<u>Kanál</u>	MQZAO_DELETE
<u>Kanál připojení klienta</u>	MQZAO_DELETE
<u>Modul listener</u>	MQZAO_DELETE
<u>Služba</u>	MQZAO_DELETE
<u>Informace o komunikaci</u>	MQZAO_DELETE

### **Zjišťovat objekt**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
<u>Fronta</u>	MQZAO_ZOBRAZENÍ
<u>Téma</u>	MQZAO_ZOBRAZENÍ
<u>Proces</u>	MQZAO_ZOBRAZENÍ
<u>správce front</u>	MQZAO_ZOBRAZENÍ
<u>Seznam názvů</u>	MQZAO_ZOBRAZENÍ
<u>Ověřovací informace</u>	MQZAO_ZOBRAZENÍ
<u>Kanál</u>	MQZAO_ZOBRAZENÍ
<u>Kanál připojení klienta</u>	MQZAO_ZOBRAZENÍ
<u>Modul listener</u>	MQZAO_ZOBRAZENÍ
<u>Služba</u>	MQZAO_ZOBRAZENÍ

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
<u>Informace o komunikaci</u>	MQZAO_ZOBRAZENÍ

**Zjišťovat názvy objektu *objekt***

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Fronta	Žádná kontrola
Téma	Žádná kontrola
Proces	Žádná kontrola
Správce front	Žádná kontrola
Seznam názvů	Žádná kontrola
Ověřovací informace	Žádná kontrola
Kanál	Žádná kontrola
Kanál připojení klienta	Žádná kontrola
Modul listener	Žádná kontrola
Služba	Žádná kontrola
<u>Informace o komunikaci</u>	Žádná kontrola

**Spustit *objekt***

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Fronta	Nelze použít
Téma	Nelze použít
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít
Ověřovací informace	Nelze použít
<u>Kanál</u>	MQZAO_CONTROL
Kanál připojení klienta	Nelze použít
<u>Modul listener</u>	MQZAO_CONTROL
<u>Služba</u>	MQZAO_CONTROL
<u>Informace o komunikaci</u>	Nelze použít

**Zastavte *objekt***

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Fronta	Nelze použít
Téma	Nelze použít
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít



<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Ověřovací informace	Nelze použít
<u>Kanál</u>	MQZAO_CONTROL
Kanál připojení klienta	Nelze použít
<u>Modul listener</u>	MQZAO_CONTROL
<u>Služba</u>	MQZAO_CONTROL
Informace o komunikaci	Nelze použít

### Příkazy kanálu

<b>Příkaz</b>	<b>Objekt</b>	<b>Je vyžadována autorizace</b>
<u>Odeslat signál Ping pro kanál</u>	Kanál	MQZAO_CONTROL
<u>Resetovat kanál</u>	Kanál	MQZAO_CONTROL_EXTENDED
<u>Vyřešit kanál</u>	Kanál	MQZAO_CONTROL_EXTENDED

### Příkazy odběrů

<b>Příkaz</b>	<b>Objekt</b>	<b>Je vyžadována autorizace</b>
<u>Změnit odběr</u>	Téma	MQZAO_CONTROL
<u>Vytvořit odběr</u>	Téma	MQZAO_CONTROL
<u>Odstranit odběr</u>	Téma	MQZAO_CONTROL
<u>Zjistit odběr</u>	Téma	MQZAO_ZOBRAZENÍ

### Příkazy pro zabezpečení

<b>Příkaz</b>	<b>Objekt</b>	<b>Je vyžadována autorizace</b>
<u>Nastavit záznam oprávnění</u>	Správce front	ZMĚNA MQZAO_CHANGE
<u>Odstranit záznam oprávnění</u>	Správce front	ZMĚNA MQZAO_CHANGE
<u>Zjistit záznamy oprávnění</u>	Správce front	MQZAO_ZOBRAZENÍ
<u>Zjistit službu ověřování oprávnění</u>	Správce front	MQZAO_ZOBRAZENÍ
<u>Zjišťovat oprávnění pro entitu</u>	Správce front	MQZAO_ZOBRAZENÍ
<u>Nastavit záznam ověření kanálu</u>	Správce front	ZMĚNA MQZAO_CHANGE
<u>Zjistit záznam ověření kanálu</u>	Správce front	MQZAO_ZOBRAZENÍ
<u>Aktualizovat zabezpečení</u>	Správce front	ZMĚNA MQZAO_CHANGE

## Stavové zobrazení

Příkaz	Objekt	Je vyžadována autorizace
<a href="#">Zjistit stav kanálu</a>	Správce front	MQZAO_ZOBRAZENÍ Všimněte si, že v přenosové frontě je vyžadováno oprávnění +inq (nebo ekvivalentně MQZAO_INQUIRE), pokud je typ kanálu CLUSSDR.
<a href="#">Dotaz na stav modulu listener kanálu</a>	Správce front	MQZAO_ZOBRAZENÍ
<a href="#">Dotaz na stav publikování/ odběru</a>	Správce front	MQZAO_ZOBRAZENÍ
<a href="#">Dotaz na stav odběru</a>	Správce front	MQZAO_ZOBRAZENÍ
<a href="#">Zjistit stav služby</a>	Správce front	MQZAO_ZOBRAZENÍ
<a href="#">Zjistit stav tématu</a>	Správce front	MQZAO_ZOBRAZENÍ

## Příkazy klastru

Příkaz	Objekt	Je vyžadována autorizace
<a href="#">Zjistit správce front klastru</a>	Správce front	MQZAO_ZOBRAZENÍ
<a href="#">Aktualizovat klastr</a>	Vyžadováno členství ve skupině 'mqm'	Vyžadováno členství ve skupině 'mqm'
<a href="#">Reset klastru</a>	Vyžadováno členství ve skupině 'mqm'	Vyžadováno členství ve skupině 'mqm'
<a href="#">Pozastavit klastr správců front</a>	Vyžadováno členství ve skupině 'mqm'	Vyžadováno členství ve skupině 'mqm'
<a href="#">Obnovit klastr správců front</a>	Vyžadováno členství ve skupině 'mqm'	Vyžadováno členství ve skupině 'mqm'

## Další administrativní příkazy

Příkaz	Objekt	Je vyžadována autorizace
<a href="#">Odeslat signál Ping pro správce front</a>	Správce front	MQZAO_ZOBRAZENÍ
<a href="#">Aktualizovat správce front</a>	Správce front	ZMĚNA MQZAO_CHANGE
<a href="#">Obnovit správce front</a>	Správce front	ZMĚNA MQZAO_CHANGE
<a href="#">Obnovit statistiku front</a>	Fronta	Funkce MQZAO_DISPLAY a MQZAO_CHANGE
<a href="#">Zjistit připojení</a>	Správce front	MQZAO_ZOBRAZENÍ
<a href="#">Zastavit připojení</a>	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 různě v různých verzích produktu Windows.

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

### **Windows** **Lokální a doménové uživatelské účty pro službu IBM MQ Windows**

Produkt IBM MQ musí během své činnosti ověřovat, zda mají ke správcům front a frontám přístup pouze autorizovaní uživatelé. To vyžaduje speciální uživatelský účet, který může produkt IBM MQ použít k dotazování na informace o každém uživateli, který se o takový přístup pokouší.

- [“Konfigurace speciálních uživatelských účtů s produktem Prepare IBM MQ Wizard” na stránce 134](#)
- [“Použití IBM MQ s Active Directory” na stránce 134](#)
- [“Uživatelská práva vyžadovaná pro službu IBM MQ Windows Service” na stránce 135](#)

## Konfigurace speciálních uživatelských účtů s produktem Prepare IBM MQ Wizard

Produkt Prepare IBM MQ Wizard vytvoří speciální uživatelský účet, aby služba Windows mohla sdílet procesy, které je potřebují používat (viz [Konfigurace produktu IBM MQ pomocí Průvodce přípravou produktu IBM MQ](#)).

Služba Windows je sdílena mezi klientskými procesy pro instalaci produktu IBM MQ . Pro každou instalaci se vytvoří jedna služba. Každá služba má název MQ\_InstallationName a má zobrazovaný název IBM MQ (InstallationName).

Vzhledem k tomu, že každá služba musí být sdílena mezi neinteraktivními a interaktivními relacemi přihlášení, musíte je spustit pod zvláštním uživatelským účtem. Pro všechny služby můžete použít jeden speciální uživatelský účet, nebo můžete vytvořit různé speciální uživatelské účty. Každý speciální uživatelský účet musí mít právo uživatele na Přihlásit se jako služba, abyste získali další informace, viz [Tabulka 14 na stránce 135](#). Pokud ID uživatele nemá oprávnění ke spuštění služby, služba se nespustí a vrátí chybu v protokolu událostí systému Windows . Zpravidla se spustí Prepare IBM MQ Wizarda nastaví se ID uživatele správně. Pokud jste však ID uživatele nakonfigurovali ručně, je možné, že budete mít problém, který je třeba vyřešit.

Když instalujete produkt IBM MQ a poprvé spustíte produkt Prepare IBM MQ Wizard , vytvoří lokální uživatelský účet pro službu s názvem MUSR\_MQADMIN s požadovanými nastaveními a oprávněními, včetně volby Logon as a service.

Pro následné instalace vytvoří produkt Prepare IBM MQ Wizard uživatelský účet s názvem MUSR\_MQADMINx, kde x je další dostupné číslo představující ID uživatele, které neexistuje. Heslo pro MUSR\_MQADMINx se náhodně vygeneruje, když se vytvoří účet, a použije se ke konfiguraci přihlašovacího prostředí pro službu. Vygenerované heslo nevyprší.

Tento účet IBM MQ není ovlivněn žádnými zásadami účtu, které jsou nastaveny na systému tak, aby požadovaly, aby byla hesla účtu změněna po určité době.

Heslo není známé mimo toto jednorázové zpracování a je uloženo pomocí operačního systému Windows v zabezpečené části registru.

## Použití IBM MQ s Active Directory

V některých konfiguracích sítě, kde jsou uživatelské účty definovány na řadičích domény, které používají adresářovou službu Active Directory , lokální uživatelský účet, pod kterým je portál IBM MQ spuštěn,

nemusí mít oprávnění, které vyžaduje k dotazování na členství ve skupinách ostatních uživatelských účtů domény. Při instalaci produktu IBM MQ identifikuje produkt Prepare IBM MQ Wizard informaci o tom, zda se jedná o tento případ, tím, že provedete testy a položíte dotazy na konfiguraci sítě.

Pokud účet lokálního uživatele, pod kterým běží IBM MQ, nemá požadované oprávnění, vyzve vás Prepare IBM MQ Wizard k zadání podrobností o účtu uživatele domény s konkrétními uživatelskými právy. Informace o tom, jak vytvořit a nastavit doménový účet domény Windows, najdete v tématu [Vytvoření a nastavení účtů domény systému Windows pro produkt IBM MQ](#). Uživatelská práva, která uživatelský účet domény vyžaduje, viz [Tabulka 14 na stránce 135](#).

Když jste zadali platné podrobnosti o účtu pro uživatelský účet domény do produktu Prepare IBM MQ Wizard, nakonfiguruje průvodce službu IBM MQ Windows, aby se spustila pod novým účtem. Podrobnosti o účtu jsou zadrženy v zabezpečené části registru a uživatelé jej nemohou číst.

Když je služba spuštěna, služba IBM MQ Windows se spustí a zůstane spuštěná tak dlouho, jak je služba spuštěna. Administrátor produktu IBM MQ, který se přihlásí na server po spuštění služby Windows, může pomocí produktu MQ Explorer spravovat správce front na serveru. Tím se připojí MQ Explorer k existujícímu procesu služby Windows. Tyto dvě akce vyžadují různé úrovně oprávnění, než budou moci pracovat:

- Proces spuštění vyžaduje oprávnění ke spuštění.
- Administrátor produktu IBM MQ vyžaduje přístupové oprávnění.

## Uživatelská práva vyžadovaná pro službu IBM MQ Windows Service

V následující tabulce jsou uvedena uživatelská práva vyžadovaná pro lokální účty a uživatelské účty domény, pod kterými je spuštěna služba Windows pro instalaci produktu IBM MQ.

<i>Tabulka 14. Uživatelská práva vyžadovaná pro službu systému IBM MQ Windows</i>	
<b>Oprávnění</b>	<b>Popis</b>
Přihlašovat se jako dávková úloha	Umožňuje spuštění služby IBM MQ Windows pod tímto uživatelským účtem.
Přihlásit jako služba.	Umožňuje uživatelům nastavit službu IBM MQ Windows tak, aby se přihlašuje pomocí konfigurovaného účtu.
Ukončit běh systému	Umožňuje službě IBM MQ Windows restartovat server, je-li konfigurován tak, aby došlo k selhání při obnově služby.
Zvýšit kvóty	Nezbytné pro volání operačního systému <code>CreateProcessAsUser</code> .
Vystupovat jako část operačního systému	Nezbytné pro volání operačního systému <code>LogonUser</code> .
Obejít kontrolu procházení	Nezbytné pro volání operačního systému <code>LogonUser</code> .
Zaměnit úroveň procesu	Nezbytné pro volání operačního systému <code>LogonUser</code> .

**Poznámka:** Práva na ladění programů mohou být zapotřebí v prostředích, kde jsou spuštěny aplikace ASP a IIS.

Uživatelský účet vaší domény musí mít tato uživatelská práva Windows nastavená jako účinná uživatelská práva, která jsou uvedena v aplikaci Lokální zásada zabezpečení. Pokud nejsou, nastavte je buď pomocí lokální aplikace zásad zabezpečení lokálně na serveru, nebo pomocí domény Aplikace zabezpečení domény v široké části.

### **Windows** Oprávnění zabezpečení serveru Windows

Instalace produktu IBM MQ se chová jinak na serveru Windows , v závislosti na tom, zda lokální uživatel nebo uživatel domény provádí instalaci.

Pokud *lokální* uživatel nainstaluje produkt IBM MQ, produkt Prepare IBM MQ Wizard zjistí, že lokální uživatel vytvořený pro službu IBM MQ Windows může načíst informace o členství ve skupině pro uživatele instalace. Produkt Prepare IBM MQ Wizard požádá uživatele o otázky o konfiguraci sítě, aby určil, zda jsou definovány jiné uživatelské účty na řadičích domény spuštěných v systému Windows 2000 nebo novějším. Je-li tomu tak, služba IBM MQ Windows musí být spuštěna pod uživatelským účtem domény s konkrétním nastavením a oprávněními. Produkt Prepare IBM MQ Wizard vyzve uživatele k zadání podrobností o účtu tohoto uživatele, jak je popsáno v tématu [Konfigurace produktu IBM MQ pomocí Průvodce přípravou produktu IBM MQ](#).

Pokud uživatel *doména* instaluje produkt IBM MQ, produkt Prepare IBM MQ Wizard zjistí, že lokální uživatel vytvořený pro službu IBM MQ Windows nemůže načíst informace o členství ve skupině pro uživatele s instalací. V takovém případě portál Prepare IBM MQ Wizard vždy vyzve uživatele k zadání podrobností o účtu domény uživatele domény, které má služba IBM MQ Windows použít.

Když služba IBM MQ Windows potřebuje použít uživatelský účet domény, IBM MQ nemůže správně fungovat, dokud nebude tento účet nakonfigurován pomocí Prepare IBM MQ Wizard. Produkt Prepare IBM MQ Wizard neumožňuje uživateli pokračovat s jinými úlohami, dokud nebude služba Windows konfigurována s vhodným účtem.

Další informace naleznete v tématu [Vytvoření a nastavení doménových účtů pro produkt IBM MQ](#).

### **Windows** Změna jména uživatele přidruženého ke službě IBM MQ

Jméno uživatele přidružené ke službě IBM MQ můžete změnit tak, že vytvoříte nový účet a zadáte jeho podrobnosti pomocí Prepare IBM MQ Wizard.

## Informace o této úloze

Když instalujete produkt IBM MQ a poprvé spustíte produkt Prepare IBM MQ Wizard , vytvoří lokální uživatelský účet pro službu s názvem MUSR\_MQADMIN. Pro následné instalace vytvoří produkt Prepare IBM MQ Wizard uživatelský účet s názvem MUSR\_MQADMINx, kde x je další dostupné číslo představující ID uživatele, které neexistuje.

Možná budete muset změnit jméno uživatele přidružené ke službě IBM MQ z MUSR\_MQADMIN nebo MUSR\_MQADMINx na něco jiného. Pokud je například správce front asociován s produktem Db2, který nepřijímá jména uživatelů s více než 8 znaky, může být nutné tuto akci provést.

## Postup

1. Vytvořte nový uživatelský účet (například **NEW\_NAME** )
2. Použijte Prepare IBM MQ Wizard k zadání podrobností nového uživatelského účtu.

### **Související informace**

[Konfigurace produktu IBM MQ pomocí Průvodce přípravou produktu IBM MQ](#)

### **Windows** Změna hesla lokálního uživatelského účtu služby IBM MQ Windows

Heslo pro účet lokálního uživatele služby IBM MQ Windows můžete změnit pomocí panelu Správa počítače.

## Informace o této úloze

Chcete-li změnit heslo lokálního uživatelského účtu služby IBM MQ Windows , proveďte následující kroky:

## Postup

1. Identifikujte uživatele, pod kterým je služba spuštěna.
2. Zastavte službu IBM MQ z panelu Správa počítače.

3. Změňte požadované heslo stejným způsobem, jako byste změnili heslo jednotlivce.
4. Přejděte na vlastnosti pro službu IBM MQ z panelu Správa počítače.
5. Vyberte stránku **Přihlásit**.
6. Potvrďte, že se uvedený název účtu shoduje s uživatelem, pro který bylo heslo změněno.
7. Zadejte heslo do polí **Heslo** a **Potvrdit heslo** a klepněte na tlačítko **OK**.

**Windows** *Změna hesla pro službu IBM MQ Windows pro instalaci spuštěnou pod uživatelským účtem domény*

Jako alternativu k použití produktu Prepare IBM MQ Wizard k zadání podrobností o účtu uživatele domény můžete použít panel Správa počítačů ke změně podrobností **Přihlásit** pro specifickou službu IBM MQ pro instalaci.

## Informace o této úloze

Je-li služba IBM MQ Windows pro instalaci spuštěna pod uživatelským účtem domény, můžete změnit heslo účtu takto:

## Postup

1. Změňte heslo pro účet domény na řadiči domény. Možná budete muset požádat administrátora domény, aby to pro vás udělal.
2. Postupujte takto, chcete-li upravit stránku **Přihlášení** pro službu IBM MQ .
  - a) Identifikujte uživatele, pod kterým je služba spuštěna.
  - b) Zastavte službu IBM MQ z panelu Správa počítače.
  - c) Změňte požadované heslo stejným způsobem, jako byste změnili heslo jednotlivce.
  - d) Přejděte na vlastnosti pro službu IBM MQ z panelu Správa počítače.
  - e) Vyberte stránku **Přihlásit**.
  - f) Potvrďte, že se uvedený název účtu shoduje s uživatelem, pro který bylo heslo změněno.
  - g) Zadejte heslo do polí **Heslo** a **Potvrdit heslo** a klepněte na tlačítko **OK**.

Uživatelský účet, který služba IBM MQ Windows spouští, provádí všechny příkazy MQSC, které jsou vydány aplikacemi uživatelského rozhraní, nebo jsou prováděny automaticky při spuštění systému, ukončení práce systému nebo zotavení služby. Tento uživatelský účet musí mít proto oprávnění k administraci produktu IBM MQ . Standardně je tento příkaz přidán do lokální skupiny mqm na serveru. Je-li toto členství odebráno, služba IBM MQ Windows nebude fungovat. Další informace o uživatelských právech najdete v tématu [“Uživatelská práva vyžadovaná pro službu IBM MQ Windows Service”](#) na stránce 135.

Pokud se vyskytne problém zabezpečení s účtem uživatele, pod kterým je služba IBM MQ Windows spuštěna, objeví se chybové zprávy a popisy v protokolu systémových událostí.

## Související informace

[Konfigurace produktu IBM MQ pomocí Průvodce přípravou produktu IBM MQ](#)

## **Windows** *Aspekty podpory serverů Windows na řadiče domény*

Při povýšení serveru Windows na řadič domény byste měli zvážit, zda je vhodné nastavení zabezpečení týkající se oprávnění uživatele a skupiny. Při změně stavu počítače Windows mezi serverem a řadičem domény byste měli vzít v úvahu, že toto může ovlivnit provoz produktu IBM MQ , protože produkt IBM MQ používá lokálně definovanou skupinu mqm.

## Nastavení zabezpečení týkající se oprávnění uživatelů domény a skupinových oprávnění

IBM MQ spoléhá na informace o členství ve skupinách k implementaci své zásady zabezpečení, což znamená, že je důležité, aby ID uživatele, které provádí operace IBM MQ, určilo členství ve skupině ostatních uživatelů.

Povýšíte-li server Windows na řadič domény, zobrazí se vám volba pro nastavení zabezpečení týkající se oprávnění uživatelů a skupin. Tato volba určuje, zda lze z aktivního adresáře načíst členství ve skupině (arbitrární). Pokud je řadič domény nastaven tak, aby lokální účty měly oprávnění k dotazování na členství ve skupinách uživatelských účtů domény, může výchozí ID uživatele vytvořené IBM MQ během instalačního procesu získat členství ve skupině pro ostatní uživatele, jak je požadováno. Je-li však řadič domény nastaven tak, aby lokální účty neměly oprávnění k dotazování na členství ve skupinách pro uživatelské účty domény, zabrání to IBM MQ provedením kontrol, že uživatelé, kteří jsou definováni v doméně, jsou autorizováni pro přístup ke správcům front nebo frontám a přístup selže. Používáte-li Windows na řadiči domény, který byl nastaven tímto způsobem, musí se použít speciální doménový uživatelský účet s požadovanými oprávněními.

V tomto případě byste měli vědět:

- Jak se chovají oprávnění zabezpečení pro vaši verzi produktu Windows .
- Jak povolit členům skupiny mqm v doméně čtení členství ve skupině.
- Jak nakonfigurovat službu IBM MQ Windows ke spuštění pod uživatelem domény.

Další informace naleznete v tématu [Konfigurace uživatelských účtů pro produkt IBM MQ](#).

### IBM MQ přístup k lokální skupině mqm

Když jsou servery Windows povýšeny na řadiče domény nebo jsou z nich vyřazovány, produkt IBM MQ ztratí přístup k lokální skupině mqm.

Je-li server povýšen na řadič domény, změní se rozsah z lokální na lokální doménu. Když je počítač degradován na server, všechny lokální skupiny domény se odeberou. To znamená, že změna počítače ze serveru na řadič domény a zpět na server ztratí přístup k lokální skupině mqm. Příznakem je chyba označující nepřítomnost lokální skupiny mqm, například:

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

Chcete-li tento problém odstranit, znovu vytvořte lokální skupinu mqm pomocí standardních nástrojů správy produktu Windows . Protože jsou všechny informace o členství ve skupinách ztraceny, musíte obnovit privilegované uživatele IBM MQ v nově vytvořené lokální skupině mqm. Je-li počítač členem domény, musíte také přidat skupinu mqm domén do lokální skupiny mqm, aby bylo možné udělit ID uživatele privilegované domény IBM MQ požadovanou úroveň oprávnění.

### **Windows** Omezení ve vnořených skupinách v systému Windows

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

Volba Active Directory může podporovat různé typy skupin v rámci kontextu domény v závislosti na funkční úrovni domény. Ve výchozím nastavení jsou domény Windows 2003 v " Windows 2000 smíšená " funkční úroveň. (Windows Server 2008 a Windows Server 2012 následujte model domény Windows 2003 .) Funkční úroveň domény určuje podporované typy skupin a úroveň vnoření povolených při konfiguraci ID uživatelů v prostředí domény. Podrobnosti o kritériích rozsahu skupiny a zařazení najdete v dokumentaci k produktu Active Directory .

Kromě požadavků Active Directory jsou uložena další omezení ID používaných produktem IBM MQ. Síťová rozhraní API používaná produktem IBM MQ nepodporují všechny konfigurace, které jsou podporovány funkční úrovní domény. V důsledku toho se produkt IBM MQ nemůže dotázat na členství ve skupině žádného ID domény přítomných v lokální skupině domény, která je poté vnořena v lokální skupině.



Navíc vícenásobné vnoření globálních a univerzálních skupin není podporováno. Jsou však podporovány okamžitě vnořené globální nebo univerzální skupiny.

## **Windows** **Autorizování uživatelů pro vzdálené použití produktu IBM MQ**

Potřebujete-li vytvořit a spustit správce front při vzdáleném připojení k produktu IBM MQ, musíte mít k dispozici uživatelský přístup Vytvořit globální objekty.

### **Informace o této úloze**

**Poznámka:** Administrátoři mají při výchozím nastavení přístup uživatele Vytvořit globální objekty, takže pokud jste administrátorem, můžete vytvářet a spouštět správce front při vzdáleném připojení, aniž by došlo ke změně vašich uživatelských práv.

Pokud se připojujete k počítači s produktem Windows pomocí služeb Terminal Services nebo Remote Desktop Connection a máte problémy s vytvářením, spouštěním nebo odstraněním správce front, může to být způsobeno tím, že nemáte přístup uživatele Vytvořit globální objekty.

Uživatelský přístup Vytvořit globální objekty omezuje uživatele, kteří mají oprávnění k vytváření objektů v globálním oboru názvů. Má-li aplikace vytvořit globální objekt, musí být buď spuštěn v globálním oboru názvů, nebo uživatel, pod kterým je spuštěna aplikace, musí mít na něj použitý uživatelský přístup Vytvořit globální objekty.

Když se připojujete vzdáleně k počítači se systémem Windows pomocí služeb Terminal Services nebo Remote Desktop Connection, aplikace běží ve svém vlastním lokálním oboru názvů. If you attempt to create or delete a queue manager using MQ Explorer or the **crtmqm** or **dltmqm** command, or to start a queue manager using the **stzmqm** command, it results in an authorization failure. Tím se vytvoří FDC IBM MQ s ID sondy XY132002.

Spuštění správce front pomocí příkazu MQ Explorernebo použití příkazu **amqmdain qmgr start** funguje správně, protože tyto příkazy přímo nespouští správce front. Místo toho příkazy odešlou požadavek na spuštění správce front do samostatného procesu spuštěného v globálním oboru názvů.

Pokud různé metody administrace IBM MQ nefungují při použití terminálových služeb, pokuste se nastavit uživatele Vytvořit globální objekty správně.

### **Postup**

1. Otevřete panel Administrativní nástroje:

#### **Windows Server 2008 a Windows Server 2012**

Tento panel otevřete pomocí nabídky **Ovládací panely > Systém a údržba > Administrativní nástroje**.

#### **Windows 8.1**

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

2. Poklepejte na položku **Lokální zásada zabezpečení**.
3. Rozbalte **Lokální zásady**.
4. Klepněte na volbu **Přiřazení práv uživatele**.
5. Přidejte nového uživatele nebo skupinu do zásady Vytvořit globální objekty.

### **Ukončovací program kanálu SSPI**

Produkt IBM MQ for Windows poskytuje uživatelský program zabezpečení, který lze použít pro kanály zpráv i pro kanály MQI. Ukončení je dodáno jako zdrojový a objektový kód a poskytuje jednosměrně a dvoucestné ověření.

Uživatelská procedura zabezpečení používá rozhraní SSPI (Security Support Provider Interface), které poskytuje integrované bezpečnostní mechanismy platforem Windows.

Uživatelská procedura zabezpečení poskytuje následující služby identifikace a ověření:



## **jednosměrné ověření**

To používá podporu ověření produktu Windows NT LAN Manager (NTLM). NTLM umožňuje serverům autentizovat své klienty. Neumožňuje klientovi ověřit identitu serveru nebo jeden server pro ověření jiného serveru. NTLM byl navržen pro síťové prostředí, ve kterém se předpokládá, že servery jsou pravé. NTLM je podporováno na všech platformách Windows, které jsou podporovány produktem IBM WebSphere MQ 7.0.

Tato služba se zpravidla používá na kanálu MQI k povolení správce front serveru pro ověření aplikace IBM MQ MQI client. Klientská aplikace je identifikována pomocí ID uživatele přidruženého k procesu, který je spuštěn.

Chcete-li provést ověření, uživatelská procedura zabezpečení na straně klienta kanálu získá token ověření z NTLM a odešle token ve zprávě zabezpečení svému partnerovi na druhém konci kanálu. Uživatelská procedura zabezpečení partnera předá token do NTLM, který kontroluje, zda je token autentický. Pokud uživatelská procedura pro zabezpečení partnera není s autenticitou tokenu spokojena, dává pokyn programu MCA k uzavření kanálu.

## **Dva způsoby, nebo vzájemné, ověření**

To používá ověřovací služby Kerberos. Protokol Kerberos nepředpokládá, že servery v síťovém prostředí jsou skutečné. Servery mohou ověřovat klienty a jiné servery a klienti mohou ověřovat servery. Kerberos je podporován na všech platformách Windows, které jsou podporovány produktem IBM WebSphere MQ 7.0.

Tuto službu lze použít pro kanály zpráv i pro kanály MQI. Na kanálu zpráv poskytuje vzájemné ověření těchto dvou správců front. Na kanálu MQI je možné, aby se správce front serveru a aplikace IBM MQ MQI client vzájemně ověřovali. Správce front je identifikován svým názvem s předponou řetězcem `ibmqSeries/`. 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](#).

## **Použití souborů šablon zabezpečení na Windows**

Použití šablony může ovlivnit nastavení zabezpečení použité pro soubory a adresáře produktu IBM MQ. Používáte-li vysoce zabezpečenou šablonu, použijte ji před instalací produktu IBM MQ.

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

Použití jedné z těchto šablon může mít vliv na nastavení zabezpečení aplikovaná na soubory a adresáře produktu IBM MQ. Chcete-li použít šablonu Vysoce Secure, nakonfigurujte počítač před instalací produktu IBM MQ.

Pokud použijete vysoce zabezpečenou šablonu na počítač, na kterém je již produkt IBM MQ nainstalován, budou odebrána všechna oprávnění, která jste nastavili u souborů a adresářů produktu IBM MQ. Protože

tato oprávnění jsou odebrána, ztratíte uživatele *Administrator*, *mqma* v případě potřeby přístup skupiny *Everyone* z chybových adresářů.

## **Konfigurace dodatečného oprávnění pro aplikace produktu Windows připojující se k produktu IBM MQ**

Účet, pod kterým mohou být spuštěny procesy produktu IBM MQ , může vyžadovat dodatečné oprávnění dříve, než může být udělen přístup k procesům aplikace SYNCHRONIZE k procesům aplikace.

### **Informace o této úloze**

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

IBM MQ vyžaduje přístup SYNCHRONIZE k procesům aplikace za účelem koordinace určitých akcí. Když se serverová aplikace nejprve pokusí připojit ke správci front IBM MQ , upraví proces tak, aby udělil oprávnění SYNCHRONIZE pro administrátory produktu IBM MQ . Avšak účet, pod kterým jsou spuštěny procesy produktu IBM MQ , může vyžadovat další oprávnění, dříve než může být udělen požadovaný přístup.

Chcete-li konfigurovat další oprávnění k ID uživatele, pod kterým jsou procesy produktu IBM MQ spuštěny, postupujte takto:

### **Postup**

1. Spusťte nástroj Lokální zásady zabezpečení, klepněte na **Nastavení zabezpečení->Lokální zásady->Přiřazení uživatele**, klepněte na **Ladit programy**.
2. Poklepejte na položku **Ladit programy** poté do seznamu přidejte ID uživatele produktu IBM MQ .

Pokud se systém nachází v doméně Windows a nastavení efektivní zásady stále není nastaveno, i když je nastaveno lokální nastavení zásad, musí být ID uživatele autorizováno stejným způsobem na úrovni domény, pomocí nástroje zásad zabezpečení domény.

## **Nastavení zabezpečení v systému HP Integrity NonStop Server**

Aspekty zabezpečení specifické pro systémy HP Integrity NonStop Server .

Klient IBM 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 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 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 MQ . Pro použití s klientskými aplikacemi produktu IBM MQ jsou podporovány pouze knihovny OpenSSL , které jsou poskytovány produktem IBM 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 ukládat. PEM je internetovým standardem pro kryptografické výměny šifrovaného textu a je specifikován v internetových RFC 1421, 1422, 1423 a 1424. IBM 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 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 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 MQ pro HP Integrity NonStop Server. Klient IBM MQ pro HP Integrity NonStop Server je testován s následujícími entropii démony:

- amqjkd0 (jak je poskytováno serverem IBM 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 v systému IBM i

Zabezpečení pro produkt IBM MQ for IBM i je implementováno pomocí zabezpečení na úrovni objektů IBM MQ Object Authority Manager (OAM) a IBM i.

Aspekty zabezpečení, které musí být provedeny při určování přístupových oprávnění k objektům produktu IBM MQ.

Při nastavování oprávnění pro uživatele ve vašem podniku je třeba zvážit následující skutečnosti:

1. Udělte a zrušte oprávnění k příkazům IBM MQ for IBM i pomocí příkazů IBM i GRTOBJAUT a RVKOBJAUT.

V knihovně produktu QMQM jsou určité objekty noncommand (\*cmd) nastaveny tak, aby měly oprávnění **\*PUBLIC** k **\*USE**. Neměňte oprávnění těchto objektů, nebo pro poskytnutí oprávnění použijte seznam oprávnění. Jakékoli nesprávné oprávnění může ohrozit funkčnost produktu IBM MQ.

2. Během instalace produktu IBM MQ for IBM i jsou vytvořeny následující speciální profily uživatelů:

### QMQM

Používá se primárně pro interní funkce produktu. Lze ji však použít ke spuštění důvěryhodných aplikací pomocí funkce MQCNO\_FASTPATH\_BINDINGS. Viz [Připojení ke správci front pomocí volání MQCONN](#).

### QMQMADM

Je použit jako skupinový profil pro administrátory produktu IBM MQ. Profil skupiny poskytuje přístup k CL příkazům a prostředkům IBM MQ.

Když používáte SBMJOB k odeslání programů, které volají příkazy IBM MQ, USER nesmí být výslovně nastaveno na QMQMADM. Místo toho nastavte USER na QMQM nebo jiný uživatelský profil, který má uvedeno QMQMADM jako skupinu.

3. Pokud odesíláte příkazy kanálu ke vzdáleným správcům front, ujistěte se, že váš profil uživatele je členem skupiny QMQMADM na cílovém systému. Seznam příkazů kanálů PCF a MQSC naleznete v příručce [IBM MQ for IBM i CL commands](#).
4. Sada skupin přidružená k uživateli je uložena do mezipaměti, když jsou autorizace skupiny vypočítány pomocí OAM.

**Všechny změny provedené v členství uživatele ve skupinách po nastavení skupiny do mezipaměti nebudou rozpoznány, dokud správce front nerestartujete nebo nespustíte příkaz RFRMQMAUT k obnovení zabezpečení.**

5. Omezte počet uživatelů, kteří mají oprávnění pracovat s příkazy, které jsou zvláště citlivé. Tyto příkazy zahrnují:
  - Vytvoření správce front zpráv ( CRTMQM )
  - Odstranit správce front zpráv ( DLTMQM )
  - Spuštění správce front zpráv ( STRMQM )
  - Ukončení správce front zpráv ( ENDMQM )
  - Spuštění příkazového serveru ( STRMQMCSVR )
  - Ukončení příkazového serveru ( ENDMQMCSVR )
6. Definice kanálů obsahují specifikaci ukončovacího programu zabezpečení. Vytvoření a úprava kanálu vyžaduje speciální ohledy. Podrobnosti o uživatelských procedurách zabezpečení jsou uvedeny v [“Přehled uživatelské procedury zabezpečení”](#) na stránce 91.
7. Je možné nahradit programy pro ukončení kanálu a spouštěcí programy spouštěčů. Za bezpečnost těchto výměn je odpovědný programátor.

## Správce oprávnění k objektu v systému IBM i

Správce oprávnění objektu (OAM) spravuje autorizace uživatelů pro manipulaci s objekty produktu IBM MQ, včetně front a definic procesů. Poskytuje také rozhraní příkazového řádku, jehož prostřednictvím můžete udělovat nebo odvolávat přístupová oprávnění k objektu pro určitou skupinu uživatelů. Rozhodnutí o povolení přístupu k prostředku je provedeno pomocí OAM a správce front toto rozhodnutí dodržuje. Pokud OAM nemůže učinit rozhodnutí, zabrání správci front přístup k tomuto prostředku.

Prostřednictvím OAM můžete řídit:

- Přístup k objektům produktu IBM MQ prostřednictvím rozhraní MQI. Když se aplikační program pokusí o přístup k objektu, OAM zkontroluje, zda má profil uživatele, zda má požadavek, oprávnění pro požadovanou operaci.

To znamená, že to znamená, že fronty a zprávy ve frontách mohou být chráněny před neoprávněným přístupem.

- Oprávnění k použití příkazů PCF a MQSC.

Různé skupiny uživatelů mohou mít různé přístupové oprávnění ke stejnému objektu. Například u určité fronty může jedna skupina provádět operace put i get; jiná skupina může být povolena pouze pro procházení fronty (MQGET s volbou procházení). Podobně, některé skupiny mohou mít oprávnění k získání a vložení do fronty, ale nejsou povoleny změny nebo odstranění fronty.

Příkazy IBM MQ for IBM i a provádění operací na objektech IBM MQ for IBM i

## Oprávnění IBM MQ v systému IBM i

Chcete-li přistupovat k objektům produktu IBM MQ, potřebujete oprávnění k vydání příkazu a k přístupu k odkazovanému objektu. Administrátoři mají přístup ke všem prostředkům produktu IBM MQ.

Přístup k objektům produktu IBM MQ je řízen oprávněními pro:

1. Zadejte příkaz IBM MQ .
2. Přístup k objektům produktu IBM MQ , na které příkaz odkazuje.

Všechny CL příkazy IBM MQ for IBM i se dodávají s vlastníkem QMQM a administrativní profil (QMADM) má oprávnění \*USE k přístupu \*PUBLIC nastaveným na \*EXCLUDE.

**Poznámka:** Program QSRDUPER je používán programem IBM MQ pro instalaci licencovaného programu IBM i pro duplikaci objektů Command (\*CMD) v QSYS. Ve verzi IBM i V5R4 a později byl program QSRDUPER změněn tak, aby předvolené chování bylo vytvořit příkaz proxy místo duplikátu původního příkazu. Příkaz proxy přesměruje provedení příkazu na jiný příkaz a má atribut PRX. Pokud příkaz proxy stejného názvu jako kopírovaný příkaz existuje v knihovně QSYS, soukromé oprávnění k příkazu proxy se neudělí příkazu v knihovně produktu. Pokusy o výzvu nebo spuštění příkazu proxy v QSYS kontrolují oprávnění cílového příkazu v knihovně produktu. Jakékoli změny v oprávnění k objektům \*CMD proto musí být provedeny v knihovně produktu (QMADM) a ty v QSYS není třeba upravovat. Příklad:

```
GRTOBJAUT OBJ(QMQM/DSPMQM) OBJTYPE(*CMD) USER(MQUSER) AUT(*USE)
```

Změny struktury oprávnění u některých CL příkazů produktu umožňují veřejné použití těchto příkazů, pokud máte požadované oprávnění OAM k objektům IBM MQ , aby tyto změny byly provedeny.

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

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

### Související pojmy

[“Oprávnění ke správě produktu IBM MQ v systému IBM i” na stránce 72](#)

## **Přístupová oprávnění pro objekty IBM MQ v systému IBM i**

Přístupové oprávnění požadované pro spuštění CL příkazů IBM MQ .

IBM MQ for IBM i kategorizuje CL příkazy produktu do dvou skupin:

### Skupina 1

Uživatelé musí být ve skupině uživatelů QMADM, nebo mít oprávnění \*ALLOBJ ke zpracování těchto příkazů. Uživatelé, kteří mají některou z těchto oprávnění, mohou zpracovat všechny příkazy ve všech kategoriích, aniž by museli vyžadovat další oprávnění.

**Poznámka:** Tyto orgány přepisují jakékoli oprávnění OAM.

Tyto příkazy lze seskupit podle následujících pokynů:

- Příkazy příkazového serveru
  - ENDMQMCSVR, Ukončení příkazového serveru IBM MQ
  - STRMQMCSVR, Spuštění příkazového serveru IBM MQ
- Příkaz obslužné rutiny fronty nedoručených zpráv
  - STRMQMDLQ, Spuštění popisovače fronty IBM MQ nedoručitelných zpráv
- Příkaz modulu listener
  - ENDMQMLSR, Ukončení modulu listener produktu IBM MQ
  - STRMQMLSR, Spuštění neobjektového modulu listener
- Příkazy obnovy médií
  - RCDMQMIMG, Záznam obrazu objektu IBM MQ
  - RCRMQMOBJ, Re-create IBM MQ Objekt

- WRKMQMTRN, práce s IBM MQ Q transakcemi
- Příkazy správce front
  - CRTMQM, Vytvoření správce front zpráv
  - DLTMQM, Výmaz správce front zpráv
  - ENDMQM, Ukončit správce front zpráv
  - STRMQM, Spuštění správce front zpráv
- Příkazy pro zabezpečení
  - GRMQMAUT, Udělení oprávnění k objektu IBM MQ
  - RVKMQMAUT, Odvolání oprávnění k objektu IBM MQ
- Příkaz trasování
  - TRCMQM, Trasování úlohy IBM MQ
- Příkazy pro transakce
  - RSVMQMTRN, Vyřešit transakci IBM MQ
- Příkazy monitoru spouštěčů
  - STRMQMTRM, Spuštění monitoru spouštěčů
- Příkazy SC produktu IBM MQ
  - RUNMQSC, spusťte příkazy produktu IBM MQSC
  - STRMQMMU, Spuštění příkazů produktu IBM MQSC

## Skupina 2

Zbývající příkazy, pro které jsou požadovány dvě úrovně oprávnění:

1. Oprávnění IBM i ke spuštění příkazu. Administrátor serveru IBM MQ jej nastavuje pomocí příkazu **GRTOBJAUT**, aby přepsal omezení \*PUBLIC pro uživatele nebo skupinu uživatelů.

Příklad:

```
GRTOBJAUT OBJ(QMQM/DSPMQMQ) OBJTYPE(*CMD) USER(MQUSER) AUT(*USE)
```

2. IBM MQ oprávnění k manipulaci s objekty IBM MQ přidruženými k příkazu nebo příkazům, s ohledem na správné oprávnění IBM i v kroku 1.

Toto oprávnění je řízeno uživatelem s příslušným oprávněním OAM pro požadovanou akci, kterou nastavil administrátor produktu IBM MQ pomocí příkazu **GRMQMAUT**.

Příklad:

```
GRMQMAUT *connect authority to the queue manager + *admchg authority to
the queue
```

Příkazy lze seskupit podle následujících pokynů:

- Příkazy kanálu
  - CHGMQMCHL, změna kanálu IBM MQ
    - To vyžaduje \* oprávnění k připojení ke správci front a \* admchg oprávnění ke kanálu.
  - CPYMQMCHL, kopírovat kanál IBM MQ
    - To vyžaduje \* connect and \* admcrct authority to the queue manager, \* admdsp authority to the default channel type to be copied, and \* admcrct authority to the channel object class.
    - Například kopírování odesílacího kanálu vyžaduje oprávnění \* admdsp na SYSTEM.DEF.SENDER
  - CRTMQMCHL, Vytvořit kanál IBM MQ

To vyžaduje \* connect and \* admcrt authority to the queue manager, \* admdsp authority to the default channel type to be created and \* admccrt authority to the channel object class.

Například vytvoření kanálu odesílatele vyžaduje oprávnění \* admdsp pro SYSTEM.DEF.SENDER

- DLTMQMCHL, Výmaz kanálu IBM MQ

To vyžaduje \* oprávnění k připojení ke správci front a \* admdlť oprávnění ke kanálu.

- RSVMSQMCHL, Vyřešit kanál IBM MQ

To vyžaduje \* oprávnění k připojení ke správci front a \* ctrlx oprávnění ke kanálu.

- Zobrazit příkazy

Chcete-li zpracovat příkazy DSP, musíte udělit uživateli oprávnění \*connect a \*admdsp správci front společně s libovolnou specifickou uvedenou volbou:

- DSPMQM, Zobrazení správce front zpráv
- DSPMQMAUT, Zobrazení oprávnění k objektu IBM MQ
- DSPMQMAUTI, Zobrazení ověřovacích informací IBM MQ - \*admdsp na objekt ověřovacích informací
- DSPMQMCHL, Zobrazení kanálu IBM MQ - \*admdsp na kanál
- DSPMQMCSV, Zobrazení příkazového serveru IBM MQ
- DSPMQMNL, Zobrazení seznamu názvů IBM MQ - \*admdsp na seznam názvů
- DSPMQMOVBN, Zobrazení názvů objektů IBM MQ
- DSPMQMPRC, Zobrazení IBM MQ procesu- \*admdsp na proces
- DSPMQMQ, Zobrazení fronty IBM MQ - \*admdsp do fronty
- DSPMQMTOP, Zobrazit téma IBM MQ - \*admdsp na téma

- Práce s příkazy

Chcete-li zpracovat příkazy WRK a zobrazit panel s volbami, musíte udělit uživateli oprávnění \*connect a \*admdsp správci front společně s libovolnou specifickou uvedenou volbou:

- WRKMQM, Práce se správci front zpráv
- WRKMQMAUT, Práce s oprávněním k objektu IBM MQ
- WRKMQMAUTD, práce s daty oprávnění k objektu IBM MQ
- WRKMQMAUTI, práce s ověřovacími informacemi IBM MQ
  - \*admchg pro příkaz Změnit objekt ověřovacích informací IBM MQ .
  - \*admcrť pro příkaz Vytvořit a kopírovat objekt ověřovacích informací IBM MQ .
  - \*admdlť pro příkaz Odstranit objekt ověřovacích informací IBM MQ .
  - \*admdsp pro příkaz Display IBM MQ Authentication Information Object.
- WRKMQMCHL, práce s kanálem IBM MQ

To vyžaduje následující oprávnění:

- \*admchg pro příkaz Změnit kanál IBM MQ .
- \*admc1x pro příkaz Clear IBM MQ Channel.
- \*admcrť pro příkaz Vytvořit a kopírovat kanál IBM MQ .
- \*admdlť pro příkaz Delete IBM MQ Channel.
- \*admdsp pro příkaz Display IBM MQ Channel.
- \*ctrl pro příkaz Start IBM MQ Channel.
- \*ctrl pro příkaz End IBM MQ Channel.
- \*ctrl pro příkaz Ping IBM MQ Channel.
- \*ctrlx pro příkaz Reset kanálu IBM MQ .

- \*ctrlx pro příkaz Vyřešit kanál IBM MQ .
- WRKMQMCHST, Práce se stavem kanálu IBM MQ
  - To vyžaduje oprávnění \*admdsp ke kanálu.
- WRKMQMCL, práce s klastry IBM MQ
- WRKMQMCLQ, Práce s frontami klastru IBM MQ
- WRKMQMCLQM, Práce se správcem front klastru IBM MQ
- WRKMQMLSR, práce s modulem listener IBM MQ
- WRKMQMMSG, Práce se zprávami IBM MQ
  - To vyžaduje oprávnění \*browse ke frontě
- WRKMQMNL, Práce s IBM MQ seznamy názvů
  - To vyžaduje následující oprávnění:
    - \*admchg pro příkaz Změna seznamu názvů IBM MQ .
    - \*admcr t pro příkaz Vytvořit a kopírovat seznam názvů IBM MQ .
    - \*admdl t pro příkaz Odstranit seznam názvů IBM MQ .
    - \*admdsp pro příkaz Zobrazení seznamu názvů IBM MQ .
- WRKMQMPCR, práce s procesy IBM MQ
  - To vyžaduje následující oprávnění:
    - \*admchg pro příkaz Změnit proces IBM MQ .
    - \*admcr t pro příkaz Vytvořit a kopírovat proces IBM MQ .
    - \*admdl t pro příkaz Odstranit proces IBM MQ .
    - \*admdsp pro příkaz Display IBM MQ Process.
- WRKMQMQ, práce s frontami IBM MQ
  - To vyžaduje následující oprávnění:
    - \*admchg pro příkaz Změnit frontu IBM MQ .
    - \*admc l r pro příkaz Vymazat frontu IBM MQ .
    - \*admcr t pro příkaz Vytvořit a kopírovat frontu IBM MQ .
    - \*admdl t pro příkaz Odstranit frontu IBM MQ .
    - \*admdsp pro příkaz Zobrazení fronty IBM MQ .
- WRKMQMQSTS, Práce se stavem fronty IBM MQ
- WRKMQMTOP, Práce s tématy IBM MQ
  - To vyžaduje následující oprávnění
    - \*admchg pro příkaz Změnit téma IBM MQ .
    - \*admcr t pro příkaz Vytvořit a kopírovat téma IBM MQ .
    - \*admdl t pro příkaz Odstranit téma IBM MQ .
    - \*admdsp pro příkaz Display IBM MQ Topic.
- WRKMQMSUB, práce s odběry IBM MQ
- Další příkazy kanálu
  - Chcete-li zpracovat příkazy kanálu, musíte udělit uživateli uvedené specifické oprávnění:
    - ENDMQMCHL, Ukončit IBM MQ kanál
      - To vyžaduje oprávnění \*connect ke správci front a oprávnění \*allmqi k přenosové frontě přidružené k kanálu.
    - ENDMQMLSR, Ukončení listeneru IBM MQ



- To vyžaduje oprávnění `*connect` ke správci front a oprávnění správce `*ctrl` k uvedenému objektu modulu listener.
- PINGMQMCHL, Ping IBM MQ kanál
  - To vyžaduje oprávnění `*connect` a `*inq` ke správci front a oprávnění správce `*ctrl` k objektu kanálu.
- RSTMQMCHL, Resetovat kanál IBM MQ
  - To vyžaduje oprávnění `*connect` ke správci front.
- STRMQMCHL, spuštění kanálu IBM MQ
  - To vyžaduje oprávnění `*connect` ke správci front a oprávnění správce `*ctrl` k objektu kanálu.
- STRMQMCHLI, Spuštění iniciátoru kanálu IBM MQ
  - To vyžaduje oprávnění `*connect` a `*inq` pro správce front a oprávnění správce `*allmqi` k inicializační frontě přidružené k přenosové frontě kanálu.
- STRMQMLSR, Spuštění modulu listener IBM MQ
  - To vyžaduje `*` oprávnění k připojení ke správci front a oprávnění `*` `ctrl` k uvedenému objektu listeneru.
- Další příkazy:
  - Chcete-li zpracovat následující příkazy, musíte udělit uživateli uvedené specifické oprávnění:
    - CCTMQM, připojte se ke správci front zpráv
      - To nevyžaduje žádné oprávnění k objektu IBM MQ .
    - CHGMQM, Změna správce front zpráv
      - To vyžaduje oprávnění `*connect` a `*admchg` ke správci front.
    - CHGMQMAUTI, změna ověřovacích informací IBM MQ
      - To vyžaduje oprávnění `*connect` ke správci front a oprávnění `*admchg` a `*admdsp` k objektu ověřovacích informací.
    - CHGMQMNL, Změna seznamu názvů IBM MQ
      - To vyžaduje oprávnění `*connect` ke správci front a oprávnění `*admchg` k seznamu názvů.
    - CHGMQMPCRC, Změna IBM MQ procesu
      - To vyžaduje oprávnění `*connect` ke správci front a oprávnění `*admchg` k procesu.
    - CHGMQMQR, Změna fronty IBM MQ
      - To vyžaduje oprávnění `*connect` ke správci front a oprávnění `*admchg` k frontě.
    - CLRMQMQR, Vymazat frontu IBM MQ
      - To vyžaduje oprávnění `*connect` ke správci front a oprávnění `*admcrl` k frontě.
    - CPYMQMAUTI, kopírování ověřovacích informací IBM MQ
      - To vyžaduje oprávnění `*connect` ke správci front a oprávnění `*admdsp` k objektu ověřovacích informací a oprávnění `*admctrl` k třídě objektů ověřovacích informací.
    - CPYMQMNL, Kopírovat seznam názvů IBM MQ
      - To vyžaduje oprávnění `*connect` a `*admctrl` ke správci front.
    - CPYMQMPCRC, kopírovat proces IBM MQ
      - To vyžaduje oprávnění `*connect` a `*admctrl` ke správci front.
    - CPYMQMQR, Kopírovat frontu IBM MQ
      - To vyžaduje oprávnění `*connect` a `*admctrl` ke správci front.
    - CRTMQMAUTI, vytvoření ověřovacích informací IBM MQ

- To vyžaduje oprávnění \*connect ke správci front a oprávnění \*admdsp k objektu ověřovacích informací a oprávnění \*admcr t k třídě objektů ověřovacích informací.
- CRTMQMNL, Vytvoření seznamu názvů IBM MQ
 

To vyžaduje oprávnění \*connect a \*admcr t pro správce front a oprávnění správce \*admdsp k výchozímu seznamu názvů.
  - CRTMQMPRC, Vytvoření procesu IBM MQ
 

To vyžaduje oprávnění \*connect a \*admcr t ke správci front a oprávnění \*admdsp k výchozímu procesu.
  - CRTMQMQ, Vytvoření fronty IBM MQ
 

To vyžaduje oprávnění \*connect a \*admcr t pro správce front a oprávnění správce \*admdsp k výchozí frontě.
  - CVTMQMDTA, Převést příkaz datového typu IBM MQ
 

To nevyžaduje žádné oprávnění k objektu IBM MQ .
  - DLTMQMAUTI, Výmaz ověřovacích informací IBM MQ
 

To vyžaduje oprávnění \*connect ke správci front a oprávnění \*ctrlx k objektu ověřovacích informací.
  - DLTMQMNL, Výmaz seznamu názvů IBM MQ
 

To vyžaduje oprávnění \*connect ke správci front a oprávnění \*admdl t k seznamu názvů.
  - DLTMQMPRC, odstranit proces IBM MQ
 

To vyžaduje oprávnění \*connect ke správci front a oprávnění \*admdl t k procesu.
  - DLTMQMQ, Výmaz fronty IBM MQ
 

To vyžaduje oprávnění \*connect ke správci front a oprávnění \*admdl t k frontě.
  - DSCMQM, odpojení od správce front zpráv
 

To nevyžaduje žádné oprávnění k objektu IBM MQ .
  - RFRMQMAUT, Aktualizovat zabezpečení
 

To vyžaduje oprávnění \*connect ke správci front.
  - RFRMQMCL, Aktualizovat klastr
 

To vyžaduje oprávnění \*connect ke správci front.
  - RSMMQMCLQM, Obnovit správce front klastru
 

To vyžaduje oprávnění \*connect ke správci front.
  - RSTMQMCL, Resetovat klastr
 

To vyžaduje oprávnění \*connect ke správci front.
  - SPDMQMCLQM, pozastavení správce front klastru
 

To vyžaduje oprávnění \*connect ke správci front.

### ***Oprávnění pro přístup k produktu IBM i***

Tyto informace vám pomohou porozumět příkazům autorizace přístupu.

Oprávnění definované klíčovým slovem AUT na příkazech GRTMQMAUT a RVKMQMAUT lze kategorizovat takto:

- Oprávnění související s voláními MQI
- Příkazy administrace související s autorizací
- Kontextové autorizace
- Obecné autorizace, tj. volání MQI, příkazů nebo obojího.

V následujících tabulkách jsou uvedeny různé oprávnění použitím parametru AUT pro volání MQI, volání kontextu, příkazy MQSC a PCF a generické operace.

<i>Tabulka 15. Oprávnění pro volání MQI</i>	
<b>AUT.</b>	<b>Popis</b>
*ALTUSR	Povolit použití oprávnění jiného uživatele pro volání MQOPEN a MQPUT1 .
*BROWSE	Načtěte zprávu z fronty zadáním volání MQGET s volbou BROWSE.
*CONNECT	Připojení aplikace k zadanému správci front zadáním volání MQCONN.
*GET	Načtení zprávy z fronty zadáním volání MQGET.
*INQ	Vytvoření dotazu pro konkrétní frontu zadáním volání MQINQ.
*PUB	Chcete-li publikovat zprávu pomocí volání MQPUT, otevřete téma.
*PUT	Vložit zprávu do určité fronty zadáním volání MQPUT.
*RESUME	Obnovte odběr pomocí volání MQSUB.
*SET	Nastavte atributy ve frontě z rozhraní MQI zadáním volání MQSET. Pokud otevřete frontu pro více voleb, musíte být autorizováni pro každý z nich.
*SUB	Vytvořit, změnit nebo obnovit odběr u tématu pomocí volání MQSUB.

<i>Tabulka 16. Autorizace pro volání kontextu</i>	
<b>AUT.</b>	<b>Popis</b>
*PASSALL	Propustit celý kontext na uvedené frontě. Všechna pole kontextu se zkopírují z původního požadavku.
*PASSID	Předat kontext identity na zadané frontě. Kontext identity je stejný jako kontext požadavku.
*SETALL	Nastavit celý kontext na zadané frontě. Toto je používáno speciálními systémovými obslužnými programy.
*SETID	Nastavit kontext identity na zadané frontě. Toto je používáno speciálními systémovými obslužnými programy.

<i>Tabulka 17. Oprávnění pro volání MQSC a PCF</i>	
<b>AUT.</b>	<b>Popis</b>
*ADMCHG	Změnit atributy uvedeného objektu.
*ADMCLR	Vymažte uvedený objekt (pouze příkaz objektu PCF Clear).
*ADMCR	Vytvořte objekty uvedeného typu.
*ADMDEL	Vymažte uvedený objekt.
*ADMDS	Zobrazí atributy uvedeného objektu.

<i>Tabulka 18. Oprávnění pro generické operace</i>	
<b>AUT.</b>	<b>Popis</b>
*ALL	Použít všechny operace použitelné pro objekt. Oprávnění all se rovná sjednocení oprávnění alladm, allmqia system odpovídající danému typu objektu.
*ALLADM	Provádět všechny administrační operace vztahující se na objekt.

Tabulka 18. Oprávnění pro generické operace (pokračování)

AUT.	Popis
*ALLMQI	Použít všechna volání MQI použitelná pro objekt.
*CTRL	Řídit spuštění a ukončení kanálů, listenerů a služeb.
*CTRLX	Obnovte pořadové číslo a vyřešte nejisté kanály.

## Použití příkazů autorizace přístupu v systému IBM i

Tyto informace použijte k získání informací o příkazech pro autorizaci přístupu a k použití příkladů příkazů.

### Použití příkazu GRMQMAUT

Pokud máte požadované oprávnění, můžete použít příkaz GRMQMAUT k udělení autorizace profilu uživatele nebo skupiny uživatelů pro přístup k určitému objektu. Následující příklady ilustrují použití příkazu GRMQMAUT :

1. 

```
GRMQMAUT OBJ(RED.LOCAL.QUEUE) OBJTYPE(*LCLQ) USER(GROUPA) +
AUT(*BROWSE *PUT) MQMNAME('saturn.queue.manager')
```

V tomto příkladu platí následující:

- RED . LOCAL . QUEUE je název objektu.
- \*LCLQ (lokální fronta) je typ objektu.
- GROUPA je jméno uživatelského profilu na systému, pro který se autorizace mění. Tento profil může být použit jako skupinový profil pro ostatní uživatele.
- \*BROWSE a \*PUT jsou autorizace, která jsou udělena pro uvedenou frontu.

Produkt \*BROWSE přidá autorizaci k procházení zpráv ve frontě (aby bylo možné zadat příkaz MQGET s volbou procházení).

Příkaz \*PUT přidá do fronty oprávnění pro vkládání zpráv (MQPUT).

- saturn . queue . manager je název správce front.
2. Následující příkaz uděluje uživatelům JACK a JACK všechny příslušné autorizace pro všechny definice procesů, pro výchozího správce front.

```
GRMQMAUT OBJ(*ALL) OBJTYPE(*PRC) USER(JACK JILL) AUT(*ALL)
```

3. Následující příkaz udělí uživateli GEORGE oprávnění k vložení zprávy do fronty ORDERSve správci front TRENT.

```
GRMQMAUT OBJ(TRENT) OBJTYPE(*MQM) USER(GEORGE) AUT(*CONNECT) MQMNAME (TRENT)
GRMQMAUT OBJ(ORDERS) OBJTYPE(*Q) USER(GEORGE) AUT(*PUT) MQMNAME (TRENT)
```

### Použití příkazu RVKMQMAUT

Máte-li požadované oprávnění, můžete pomocí příkazu RVKMQMAUT odebrat dříve udělené oprávnění profilu uživatele nebo skupiny uživatelů pro přístup k určitému objektu. Následující příklady ilustrují použití příkazu RVKMQMAUT :

1. 

```
RVKMQMAUT OBJ(RED.LOCAL.QUEUE) OBJTYPE(*LCLQ) USER(GROUPA) +
AUT(*PUT) MQMNAME('saturn.queue.manager')
```

Oprávnění k vložení zpráv do zadané fronty, které bylo uděleno v předchozím příkladu, je odebráno pro GROUPA.

2.

```
RVKMQMAUT OBJ(PAY*) OBJTYPE(*Q) USER(*PUBLIC) AUT(*GET) +
MQMNAME(PAYROLLQM)
```

Oprávnění k získání zpráv z libovolné fronty s názvem začínajícím znaky PAY vlastněnými správcem front PAYROLLQM je odebráno ze všech uživatelů systému, pokud tyto osoby nebo skupina, do které patří, nebyly samostatně autorizovány.

## Použití příkazu DSPMQMAUT

Zobrazení oprávnění MQM ( DSPMQMAUT ) uvádí, pro uvedený objekt a uživatele, seznam oprávnění, která má uživatel pro daný objekt. Následující příklad ukazuje, jak se příkaz používá:

```
DSPMQMAUT OBJ(ADMINNL) OBJTYPE(*NMLIST) USER(JOE) OUTPUT(*PRINT) +
MQMNAME(ADMINQM)
```

## Použití příkazu RFRMQMAUT

Aktualizace zabezpečení MQM ( RFRMQMAUT ) příkaz umožňuje okamžitou aktualizaci informací o skupině autorizace produktu OAM, což odráží změny provedené na úrovni operačního systému, aniž by bylo nutné zastavit a znovu spustit správce front. Následující příklad ukazuje, jak se příkaz používá:

```
RFRMQMAUT MQMNAME(ADMINQM)
```

## Tabulky specifikací autorizace pro produkt IBM i

Pomocí těchto informací můžete určit, která autorizace je nezbytná pro použití konkrétních volání rozhraní API, a konkrétní volby těchto volání, objektů fronty, objektů procesu a objektů správce front.

Tabulky specifikace autorizace začínající v produktu [Tabulka 19 na stránce 153](#) definují přesně, jak fungují autorizace, a omezení, která platí. Tabulky se vztahují na tyto situace:

- Aplikace, které vydávají volání MQI
- Administrační programy, které vydávají příkazy MQSC jako escape PCF
- Administrační programy, které vydávají příkazy PCF

V tomto oddílu jsou informace prezentovány jako sada tabulek, které určují následující údaje:

### Akce, která se má provést

Volba MQI, příkaz MQSC nebo příkaz PCF.

### Objekt řízení přístupu

Queue, process definition, queue manager, namelist, channel, client connection channel, listener, service, or authentication information object.

### Je vyžadována autorizace

Vyjádřeno jako konstanta MQZAO\_.

V tabulkách odpovídají předponě předpony MQZAO\_ korespondující s klíčovými slovy v seznamu oprávnění pro příkazy GRTMQMAUT a RVKMQMAUT pro konkrétní entitu. Například MQZA\_BROWSE odpovídá klíčovému slovu \*BROWSE ; Podobně klíčové slovo MQZAO\_SET\_ALL\_CONTEXT odpovídá klíčovému slovu \*SETALL a tak dále. Tyto konstanty jsou definovány v souboru záhlaví cmqzc.h, který se dodává spolu s produktem.

## Autorizace MQI

Aplikace může vydat specifická volání a volby MQI pouze v případě, že je daný identifikátor uživatele, pod kterým je spuštěn (nebo jehož autorizace lze předpokládat), udělena příslušná autorizace.

Čtyři volání MQI vyžadují kontroly autorizace: MQCONN, MQOPEN, 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 rozpoznání názvu, který není alias správce front, pokud definice aliasu správce front není otevřena přímo; to znamená, že jeho název je zobrazen v poli *ObjectName* deskriptoru objektu. Oprávnění je vždy třeba pro otevřený objekt. V některých případech je vyžadováno další oprávnění nezávislé na frontě, získané prostřednictvím autorizace pro objekt správce front.

Tabulka 19 na stránce 153, Tabulka 20 na stránce 153, Tabulka 21 na stránce 154a Tabulka 22 na stránce 154 sumarizují oprávnění potřebná pro každé volání.

**Poznámka:** Tyto tabulky neuvádějí názvy seznamů názvů, kanálů, kanálů připojení klienta, modulů listener, služeb nebo objektů ověřovacích informací. Důvodem je to, že se na tyto objekty nevztahují žádná oprávnění, s výjimkou MQOO\_INQUIRE, pro které platí stejná oprávnění jako pro ostatní objekty.

<i>Tabulka 19. Autorizace zabezpečení potřebná pro volání MQCONN</i>			
<b>Je vyžadována autorizace pro:</b>	<b>Objekt fronty ( "1" na stránce 154 )</b>	<b>Objekt procesu</b>	<b>Objekt správce front</b>
Volba MQCONN	Nelze použít	Nelze použít	MQZAO_PŘIPOJENÍ

<i>Tabulka 20. Autorizace zabezpečení potřebná pro volání MQOPEN</i>			
<b>Je vyžadována autorizace pro:</b>	<b>Objekt fronty ( "1" na stránce 154 )</b>	<b>Objekt procesu</b>	<b>Objekt správce front</b>
MQO_DOTAZAT SE	MQZAO_INQUIRE ( "2" na stránce 155 )	MQZAO_INQUIRE ( "2" na stránce 155 )	MQZAO_INQUIRE ( "2" na stránce 155 )
MQOOK_BROWSE	MQZAO_BROWSE	Nelze použít	Žádná kontrola
MQO_INPUT_*	MQZAO_VSTUP	Nelze použít	Žádná kontrola
MQOO_SAVE_ALL_CONTEXT ( "3" na stránce 155 )	MQZAO_VSTUP	Nelze použít	Nelze použít
MQOO_OUTPUT (normální fronta) ( "4" na stránce 155 )	MQZAO_VÝSTUP	Nelze použít	Nelze použít
MQOO_PASS_IDENTITY_CONTEXT ( "5" na stránce 155 )	MQZAO_PASS_IDENTITY_CONTEXT	Nelze použít	Žádná kontrola
MQOO_PASS_ALL_CONTEXT ( "5" na stránce 155, "6" na stránce 155 )	MQZAO_PASS_ALL_CONTEXT	Nelze použít	Žádná kontrola
MQOO_SET_IDENTITY_CONTEXT ( "5" na stránce 155, "6" na stránce 155 )	MQZAO_SET_IDENTITY_CONTEXT	Nelze použít	MQZA_SET_IDENTITY_CONTEXT ( "7" na stránce 155 )
MQOO_SET_ALL_CONTEXT ( "5" na stránce 155, "8" na stránce 155 )	MQZAO_SET_ALL_CONTEXT	Nelze použít	MQZA_SET_ALL_CONTEXT ( "7" na stránce 155 )

<i>Tabulka 20. Autorizace zabezpečení potřebná pro volání MQOPEN (pokračování)</i>			
<b>Je vyžadována autorizace pro:</b>	<b>Objekt fronty ( “1” na stránce 154 )</b>	<b>Objekt procesu</b>	<b>Objekt správce front</b>
MQOO_OUTPUT (Přenosová fronta) ( “9” na stránce 155 )	MQZAO_SET_ALL_CONTEXT	Nelze použít	MQZA_SET_ALL_CONTEXT ( “7” na stránce 155 )
MQOOK_SADA	MQZAO_SADA	Nelze použít	Žádná kontrola
MQO_ALTERNATE_USER_AUTHORITY	( “10” na stránce 155 )	( “10” na stránce 155 )	MQZAO_ALTERNATE_USER_AUTHORITY ( “10” na stránce 155, “11” na stránce 155 )

<i>Tabulka 21. Autorizace zabezpečení potřebná pro volání MQPUT1</i>			
<b>Je vyžadována autorizace pro:</b>	<b>Objekt fronty ( “1” na stránce 154 )</b>	<b>Objekt procesu</b>	<b>Objekt správce front</b>
KONTEXT MQPMO_PASS_IDENTITY_CONTEXT	MQZA_PASS_IDENTITY_CONTEXT ( “12” na stránce 155 )	Nelze použít	Žádná kontrola
MQPMO_PASS_ALL_CONTEXT	MQZA_PASS_ALL_CONTEXT ( “12” na stránce 155 )	Nelze použít	Žádná kontrola
KONTEXT MQPMO_SET_IDENTITY_CONTEXT	MQZA_SET_IDENTITY_CONTEXT ( “12” na stránce 155 )	Nelze použít	MQZA_SET_IDENTITY_CONTEXT ( “7” na stránce 155 )
MQPMO_SET_ALL_CONTEXT	MQZA_SET_ALL_CONTEXT ( “12” na stránce 155 )	Nelze použít	MQZA_SET_ALL_CONTEXT ( “7” na stránce 155 )
(Přenosová fronta) ( “9” na stránce 155 )	MQZAO_SET_ALL_CONTEXT	Nelze použít	MQZA_SET_ALL_CONTEXT ( “7” na stránce 155 )
MQPMO_ALTERNATE_USER_AUTHORITY	( “13” na stránce 155 )	Nelze použít	MQZAO_ALTERNATE_USER_AUTHORITY ( “11” na stránce 155 )

<i>Tabulka 22. Autorizace zabezpečení potřebná pro volání MQCLOSE</i>			
<b>Je vyžadována autorizace pro:</b>	<b>Objekt fronty ( “1” na stránce 154 )</b>	<b>Objekt procesu</b>	<b>Objekt správce front</b>
MQCO_DELETE	MQZAO_DELETE ( “14” na stránce 155 )	Nelze použít	Nelze použít
VYPRÁZDNIT ODSTRANĚNÍ MQCO_DELETE	MQZAO_DELETE ( “14” na stránce 155 )	Nelze použít	Nelze použít

**Poznámky k tabulkám:**

1. Otevírá-li se modelová fronta:

- Pro modelovou frontu je zapotřebí oprávnění MQZAO\_DISPLAY, kromě oprávnění k otevření modelové fronty pro typ přístupu, pro který se otevíráte.

- Oprávnění MQZAO\_CREATE není k vytvoření dynamické fronty zapotřebí.
  - Identifikátor uživatele použitý k otevření modelové fronty má automaticky udělena všechna oprávnění specifická pro danou frontu (ekvivalent MQZAO\_ALL) pro vytvořenou dynamickou frontu.
2. Objekt správce front, proces, seznam názvů nebo objekt správce front je kontrolován v závislosti na typu otevíraný objektu.
  3. Musí být zadán také parametr MQOO\_INPUT\_\*. Tato volba je platná pro lokální, modelovou nebo alias frontu.
  4. Tato kontrola se provádí pro všechny výstupní případy s výjimkou případu uvedeného v poznámce “9” na stránce 155.
  5. Musí být zadán také parametr MQOO\_OUTPUT.
  6. Tuto volbu má také implikovaná hodnota MQO\_P\_PASS\_IDENTITY\_CONTEXT.
  7. Toto oprávnění je povinné jak pro objekt správce front, tak pro konkrétní frontu.
  8. Tato volba předpokládá také MQOO\_PASS\_IDENTITY\_CONTEXT, MQOO\_PASS\_ALL\_CONTEXT a MQOO\_SET\_IDENTITY\_CONTEXT.
  9. Tato kontrola se provádí pro lokální nebo modelovou frontu, která má atribut fronty Usage MQUS\_TRANSMISSION, a je otevírány přímo pro výstup. Nepoužije se, je-li otevřena vzdálená fronta (buď určením názvů vzdáleného správce front a vzdálené fronty, nebo zadáním názvu lokální definice vzdálené fronty).
  10. Musí být zadán také alespoň jeden z příkazů MQOO\_INQUIRE (pro každý typ objektu) nebo MQO\_BROWSE, MQOO\_INPUT\_\*, MQOO\_OUTPUT nebo MQOO\_SET. U provedených kontrol je k dispozici kontrola ostatních voleb s použitím dodaného alternativního identifikátoru uživatele pro specifické oprávnění k objektu a aktuálního oprávnění aplikace pro kontrolu MQZAALTERNATE\_USER\_IDENTIFIER.
  11. Toto oprávnění umožňuje zadat jakékoli *AlternateUserId*.
  12. Kontrola MQZAO\_OUTPUT se provádí také tehdy, pokud fronta nemá atribut fronty Usage MQUS\_TRANSMISSION.
  13. U provedených kontrol se používají další zadané volby za použití poskytnutého alternativního identifikátoru uživatele pro uvedené oprávnění fronty a aktuální oprávnění aplikace pro kontrolu MQZAALTERNATE\_USER\_IDENTIFIER MQZAO\_ALTERNATE\_USER\_IDENTIFIER.
  14. Kontrola se provádí pouze v případě, že jsou splněny obě následující podmínky:
    - Trvalá dynamická fronta se zavírá a odstraňuje.
    - Fronta nebyla vytvořena pomocí operace MQOPEN, která vrátila použitou obsluhu objektu.
 Jinak žádná kontrola neexistuje.

### Obecné poznámky:

1. Speciální autorizace MQZAO\_ALL\_MQI obsahuje všechny následující autorizace, které jsou relevantní pro daný typ objektu:
  - MQZAO\_PŘIPOJENÍ
  - MQZAO\_DOTÁZAT SE
  - MQZAO\_SADA
  - MQZAO\_BROWSE
  - MQZAO\_VSTUP
  - MQZAO\_VÝSTUP
  - KONTEXT MQZAO\_PASS\_IDENTITY\_CONTEXT
  - MQZAO\_PASS\_ALL\_CONTEXT
  - KONTEXT MQZAO\_SET\_IDENTITY\_CONTEXT
  - FUNKCE MQZAO\_SET\_ALL\_CONTEXT
  - MQZAO\_ALTERNATE\_USER\_AUTHORITY



2. MQZAO\_DELETE (viz poznámka “14” na stránce 155 ) a MQZAO\_DISPLAY jsou klasifikovány jako autorizace pro administraci. Nejsou proto zahrnuty do struktury MQZAO\_ALL\_MQI.
3. *Žádná kontrola* znamená, že není prováděna žádná kontrola autorizace.
4. *Nepoužije se* znamená, že kontrola autorizace není pro tuto operaci relevantní. Například nemůžete vydat volání MQPUT pro objekt procesu.

### **Oprávnění pro příkazy MQSC v řídicích PCF na serveru IBM i**

Tato oprávnění umožňují uživateli zadávat příkazy administrace jako řídicí dokument PCF. Tyto metody umožňují programu odeslat administrační příkaz jako zprávu správci front za účelem jeho provedení jménem tohoto uživatele.

Tato sekce shrnuje oprávnění potřebná pro každý příkaz MQSC obsažený v Escape PCF.

*Nepoužije se* znamená, že kontrola autorizace není pro tuto operaci relevantní.

ID uživatele, pod kterým je spuštěn program, který spouští příkaz, musí mít také následující oprávnění:

- Oprávnění MQZAO\_CONNECT pro správce front
- Oprávnění DISPLAY pro správce front za účelem provedení příkazu PCF
- Oprávnění k vydávání příkazů MQSC v textu příkazu Escape PCF

#### **ALTER objekt**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Fronta	ZMĚNA MQZAO_CHANGE
Téma	ZMĚNA MQZAO_CHANGE
Proces	ZMĚNA MQZAO_CHANGE
Správce front	ZMĚNA MQZAO_CHANGE
Seznam názvů	ZMĚNA MQZAO_CHANGE
Ověřovací informace	ZMĚNA MQZAO_CHANGE
Kanál	ZMĚNA MQZAO_CHANGE
Kanál připojení klienta	ZMĚNA MQZAO_CHANGE
Modul listener	ZMĚNA MQZAO_CHANGE
Služba	ZMĚNA MQZAO_CHANGE

#### **CLEAR objekt**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Fronta	MQZAO_CLEAR
Téma	MQZAO_CLEAR
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít
Ověřovací informace	Nelze použít
Kanál	Nelze použít
Kanál připojení klienta	Nelze použít
Modul listener	Nelze použít

Objekt	Je vyžadována autorizace
Služba	Nelze použít

**DEFINE objekt NOREPLACE ( “1” na stránce 160 )**

Objekt	Je vyžadována autorizace
Fronta	MQZAO_CREATE ( “2” na stránce 160 )
Téma	MQZAO_CREATE ( “2” na stránce 160 )
Proces	MQZAO_CREATE ( “2” na stránce 160 )
Správce front	Nelze použít
Seznam názvů	MQZAO_CREATE ( “2” na stránce 160 )
Ověřovací informace	MQZAO_CREATE ( “2” na stránce 160 )
Kanál	MQZAO_CREATE ( “2” na stránce 160 )
Kanál připojení klienta	MQZAO_CREATE ( “2” na stránce 160 )
Modul listener	MQZAO_CREATE ( “2” na stránce 160 )
Služba	MQZAO_CREATE ( “2” na stránce 160 )

**DEFINE objekt REPLACE ( “1” na stránce 160, “3” na stránce 160 )**

Objekt	Je vyžadována autorizace
Fronta	ZMĚNA MQZAO_CHANGE
Téma	ZMĚNA MQZAO_CHANGE
Proces	ZMĚNA MQZAO_CHANGE
Správce front	Nelze použít
Seznam názvů	ZMĚNA MQZAO_CHANGE
Ověřovací informace	ZMĚNA MQZAO_CHANGE
Kanál	ZMĚNA MQZAO_CHANGE
Kanál připojení klienta	ZMĚNA MQZAO_CHANGE
Modul listener	ZMĚNA MQZAO_CHANGE
Služba	ZMĚNA MQZAO_CHANGE

**DELETE objekt**

Objekt	Je vyžadována autorizace
Fronta	MQZAO_DELETE
Téma	MQZAO_DELETE
Proces	MQZAO_DELETE
Správce front	Nelze použít
Seznam názvů	MQZAO_DELETE
Ověřovací informace	MQZAO_DELETE
Kanál	MQZAO_DELETE

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Kanál připojení klienta	MQZAO_DELETE
Modul listener	MQZAO_DELETE
Služba	MQZAO_DELETE

#### **DISPLAY objekt**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
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	
Služba	

#### **Odeslat signál Ping pro kanál**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Fronta	Nelze použít
Téma	Nelze použít
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít
Ověřovací informace	Nelze použít
Kanál	MQZAO_CONTROL
Kanál připojení klienta	Nelze použít
Modul listener	Nelze použít
Služba	Nelze použít

#### **Resetovat kanál**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Fronta	Nelze použít
Téma	Nelze použít
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Ověřovací informace	Nelze použít
Kanál	MQZAO_CONTROL_EXTENDED
Kanál připojení klienta	Nelze použít
Modul listener	Nelze použít
Služba	Nelze použít

### **Vyřešit kanál**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Fronta	Nelze použít
Téma	Nelze použít
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít
Ověřovací informace	Nelze použít
Kanál	MQZAO_CONTROL_EXTENDED
Kanál připojení klienta	Nelze použít
Modul listener	Nelze použít
Služba	Nelze použít

### **START objekt**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Fronta	Nelze použít
Téma	Nelze použít
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít
Ověřovací informace	Nelze použít
Kanál	MQZAO_CONTROL
Kanál připojení klienta	Nelze použít
Modul listener	MQZAO_CONTROL
Služba	MQZAO_CONTROL

### **STOP objekt**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Fronta	Nelze použít
Téma	Nelze použít
Proces	Nelze použít

Objekt	Je vyžadována autorizace
Správce front	Nelze použít
Seznam názvů	Nelze použít
Ověřovací informace	Nelze použít
Kanál	MQZAO_CONTROL
Kanál připojení klienta	Nelze použít
Modul listener	MQZAO_CONTROL
Služba	MQZAO_CONTROL

#### Poznámka:

1. Pro příkazy DEFINE je pro objekt LIKE také zapotřebí oprávnění MQZAO\_DISPLAY, je-li zadán, nebo na příslušném SYSTEM.DEFAULT.xxx , je-li LIKE vynechán.
2. Oprávnění CREATE MQZAO\_CREATE není specifické pro konkrétní objekt nebo typ objektu. Oprávnění k vytvoření je uděleno pro všechny objekty pro určitého správce front, zadáním typu objektu QMGR v příkazu GRTRMQMAUT .
3. Tato volba se použije, pokud objekt, který má být nahrazen, již existuje. Pokud tomu tak není, kontrola je určena pro atribut DEFINE *objekt* NOREPLACE.

#### **Oprávnění pro příkazy PCF na systému IBM i**

Tato oprávnění umožňují uživateli zadávat příkazy administrace jako příkazy PCF. Tyto metody umožňují programu odeslat administrační příkaz jako zprávu správci front za účelem jeho provedení jménem tohoto uživatele.

Tato sekce shrnuje oprávnění potřebná pro každý příkaz PCF.

*Žádná kontrola* znamená, že není prováděna žádná kontrola autorizace; *Nepoužije se* znamená, že kontrola autorizace není pro tuto operaci relevantní.

ID uživatele, pod kterým je spuštěn program, který spouští příkaz, musí mít také následující oprávnění:

- Oprávnění MQZAO\_CONNECT pro správce front
- Oprávnění DISPLAY pro správce front za účelem provedení příkazu PCF

Speciální autorizace MQZAO\_ALL\_ADMIN zahrnuje následující autorizace:

- ZMĚNA MQZAO\_CHANGE
- MQZAO\_CLEAR
- MQZAO\_DELETE
- MQZAO\_ZOBRAZENÍ
- MQZAO\_CONTROL
- MQZAO\_CONTROL\_EXTENDED

Objekt MQZAO\_CREATE není zahrnut, protože není specifický pro konkrétní objekt nebo typ objektu.

#### **Změna objekt**

Objekt	Je vyžadována autorizace
Fronta	ZMĚNA MQZAO_CHANGE
Téma	ZMĚNA MQZAO_CHANGE
Proces	ZMĚNA MQZAO_CHANGE
Správce front	ZMĚNA MQZAO_CHANGE

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Seznam názvů	ZMĚNA MQZAO_CHANGE
Ověřovací informace	ZMĚNA MQZAO_CHANGE
Kanál	ZMĚNA MQZAO_CHANGE
Kanál připojení klienta	ZMĚNA MQZAO_CHANGE
Modul listener	ZMĚNA MQZAO_CHANGE
Služba	ZMĚNA MQZAO_CHANGE

#### **Vymazat objekt**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
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

#### **Kopírování objekt (bez náhrady) ( "1" na stránce 166 )**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Fronta	MQZAO_CREATE ( "2" na stránce 166 )
Téma	MQZAO_CREATE ( "2" na stránce 166 )
Proces	MQZAO_CREATE ( "2" na stránce 166 )
Správce front	Nelze použít
NamelistMQZAO_VYTVORENÍ	MQZAO_CREATE ( "2" na stránce 166 )
Ověřovací informace	MQZAO_CREATE ( "2" na stránce 166 )
Kanál	MQZAO_CREATE ( "2" na stránce 166 )
Kanál připojení klienta	MQZAO_CREATE ( "2" na stránce 166 )
Modul listener	MQZAO_CREATE ( "2" na stránce 166 )
Služba	MQZAO_CREATE ( "2" na stránce 166 )

#### **Kopírování objekt (s nahrazením) ( "1" na stránce 166, "4" na stránce 166 )**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Fronta	ZMĚNA MQZAO_CHANGE
Téma	ZMĚNA MQZAO_CHANGE

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
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

**Vytvoření objektu (bez náhrady) ( “3” na stránce 166 )**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Fronta	MQZAO_CREATE ( “2” na stránce 166 )
Téma	MQZAO_CREATE ( “2” na stránce 166 )
Proces	MQZAO_CREATE ( “2” na stránce 166 )
Správce front	Nelze použít
Seznam názvů	MQZAO_CREATE ( “2” na stránce 166 )
Ověřovací informace	MQZAO_CREATE ( “2” na stránce 166 )
Kanál	MQZAO_CREATE ( “2” na stránce 166 )
Kanál připojení klienta	MQZAO_CREATE ( “2” na stránce 166 )
Modul listener	ZMĚNA MQZAO_CHANGE
Služba	ZMĚNA MQZAO_CHANGE

**Vytvořte objekt (s nahrazením) ( “3” na stránce 166, “4” na stránce 166 )**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Fronta	ZMĚNA MQZAO_CHANGE
Téma	ZMĚNA MQZAO_CHANGE
Proces	ZMĚNA MQZAO_CHANGE
Správce front	Nelze použít
Seznam názvů	ZMĚNA MQZAO_CHANGE
Ověřovací informace	ZMĚNA MQZAO_CHANGE
Kanál	ZMĚNA MQZAO_CHANGE
Kanál připojení klienta	ZMĚNA MQZAO_CHANGE
Modul listener	ZMĚNA MQZAO_CHANGE
Služba	ZMĚNA MQZAO_CHANGE

**Odstranit objekt**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Fronta	MQZAO_DELETE
Téma	MQZAO_DELETE
Proces	MQZAO_DELETE
Správce front	MQZAO_DELETE
Seznam názvů	MQZAO_DELETE
Ověřovací informace	MQZAO_DELETE
Kanál	MQZAO_DELETE
Kanál připojení klienta	MQZAO_DELETE
Modul listener	MQZAO_DELETE
Služba	MQZAO_DELETE

**Zjišťovat objekt**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Fronta	MQZAO_ZOBRAZENÍ
Téma	MQZAO_ZOBRAZENÍ
Proces	MQZAO_ZOBRAZENÍ
Správce front	MQZAO_ZOBRAZENÍ
Seznam názvů	MQZAO_ZOBRAZENÍ
Ověřovací informace	MQZAO_ZOBRAZENÍ
Kanál	MQZAO_ZOBRAZENÍ
Kanál připojení klienta	MQZAO_ZOBRAZENÍ
Modul listener	MQZAO_ZOBRAZENÍ
Služba	MQZAO_ZOBRAZENÍ

**Zjišťovat názvy objektu objekt**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Fronta	Žádná kontrola
Téma	Žádná kontrola
Proces	Žádná kontrola
Správce front	Žádná kontrola
Seznam názvů	Žádná kontrola
Ověřovací informace	Žádná kontrola
Kanál	Žádná kontrola
Kanál připojení klienta	Žádná kontrola
Modul listener	Žádná kontrola



<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Služba	Žádná kontrola

#### Odeslat signál Ping pro kanál

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Fronta	Nelze použít
Téma	Nelze použít
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít
Ověřovací informace	Nelze použít
Kanál	MQZAO_CONTROL
Kanál připojení klienta	Nelze použít
Modul listener	Nelze použít
Služba	Nelze použít

#### Resetovat kanál

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Fronta	Nelze použít
Téma	Nelze použít
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít
Ověřovací informace	Nelze použít
Kanál	MQZAO_CONTROL_EXTENDED
Kanál připojení klienta	Nelze použít
Modul listener	Nelze použít
Služba	Nelze použít

#### Obnovit statistiku front

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Fronta	Funkce MQZAO_DISPLAY a MQZAO_CHANGE
Téma	Nelze použít
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít
Ověřovací informace	Nelze použít
Kanál	Nelze použít

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Kanál připojení klienta	Nelze použít
Modul listener	
Služba	

#### **Vyřešit kanál**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Fronta	Nelze použít
Téma	Nelze použít
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít
Ověřovací informace	Nelze použít
Kanál	MQZAO_CONTROL_EXTENDED
Kanál připojení klienta	Nelze použít
Modul listener	Nelze použít
Služba	Nelze použít

#### **Spustit kanál**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Fronta	Nelze použít
Téma	Nelze použít
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít
Ověřovací informace	Nelze použít
Kanál	MQZAO_CONTROL
Kanál připojení klienta	Nelze použít
Modul listener	Nelze použít
Služba	Nelze použít

#### **Ukončit kanál**

<b>Objekt</b>	<b>Je vyžadována autorizace</b>
Fronta	Nelze použít
Téma	Nelze použít
Proces	Nelze použít
Správce front	Nelze použít
Seznam názvů	Nelze použít

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

#### Poznámka:

1. Pro příkazy Kopírovat je oprávnění MQZAO\_DISPLAY také potřebné pro objekt From.
2. Oprávnění CREATE MQZAO\_CREATE není specifické pro konkrétní objekt nebo typ objektu. Oprávnění k vytvoření je uděleno pro všechny objekty pro určitého správce front, zadáním typu objektu QMGR v příkazu GRTRMQMAUT .
3. Pro příkazy Create je zapotřebí oprávnění MQZAO\_DISPLAY také pro příslušný SYSTEM.DEFAULT.\* objekt.
4. Tato volba se použije, pokud objekt, který má být nahrazen, již existuje. Pokud tomu tak není, je kontrola funkce Kopírovat nebo Vytvořit bez náhrady.

## Generické profily OAM v systému IBM i

Generické profily správce oprávnění k objektu (OAM) vám umožňují nastavit oprávnění, které má uživatel k mnoha objektům najednou, místo toho, abyste museli vydávat samostatné příkazy **GRTRMQMAUT** pro každý jednotlivý objekt, když je vytvářen. Použití generických profilů v příkazu **GRTRMQMAUT** vám umožňují nastavit generické oprávnění pro všechny budoucí vytvořené objekty, které jsou vhodné pro daný profil.

Zbývající část tohoto oddílu popisuje použití generických profilů podrobněji:

- [“Použití zástupných znaků”](#) na stránce 166
- [“Priority profilu”](#) na stránce 167

### Použití zástupných znaků

Co znamená, že generický profil je použitím speciálních znaků (zástupné znaky) v názvu profilu. Zástupný znak otazníku (?) se například shoduje s libovolným znakem v názvu. Pokud tedy zadáte ABC . ?EF, autorizace, kterou poskytnete tomuto profilu, se vztahuje na všechny objekty vytvořené s názvy ABC . DEF, ABC . CEF, ABC . BEFatd.

Dostupné zástupné znaky jsou:

?

Otazník (?) zastupuje libovolný jeden znak. Například AB . ?D by se vztahovala na objekty AB . CD, AB . EDa AB . FD.

\*

Použijte hvězdičku (\*) jako:

- *Kvalifikátor* v názvu profilu, který odpovídá libovolnému kvalifikátoru v názvu objektu. Kvalifikátor je část názvu objektu oddělená tečkou. Název objektu ABC . DEF . GHI se například skládá z kvalifikátorů ABC, DEF a GHI.

Například ABC . \* . JKL by se vztahovala na objekty ABC . DEF . JKL a ABC . GHI . JKL. (Všimněte si, že by se **nevztahovalo** na ABC . JKL ; \* použitý v tomto kontextu vždy označuje jeden kvalifikátor.)

- Znak uvnitř kvalifikátoru v názvu profilu, který odpovídá žádnému znaku nebo více znakům v rámci kvalifikátoru ve jménu objektu.

Například ABC . DE\* . JKL by se vztahovala na objekty ABC . DE . JKL, ABC . DEF . JKL a ABC . DEGH . JKL.

**\*\***

Použijte dvojité hvězdičky (**\*\***) *jednou* v názvu profilu jako:

- Celý název profilu, který odpovídá všem názvům objektů. Pokud například použijete klíčové slovo OBJTYPE (\*PRC) k identifikaci procesů, pak jako název profilu použijte **\*\* \*\***, změníte oprávnění pro všechny procesy.
- Jako počáteční, střední nebo koncový kvalifikátor v názvu profilu odpovídá jednomu nebo více kvalifikátorům v názvu objektu. Například, **\*\***.ABC identifikuje všechny objekty s konečným kvalifikátorem ABC.

## Priority profilu

Důležitým bodem pro pochopení použití generických profilů je priorita, která jsou při rozhodování o tom, jaká oprávnění mají být použita na vytvářený objekt, upřednostňována. Předpokládejme například, že jste tyto příkazy zadali:

```
GRTMQMAUT OBJ(AB.*) OBJTYPE(*Q) USER(FRED) AUT(*PUT) MQMNAME(MYQMGR)
GRTMQMAUT OBJ(AB.C*) OBJTYPE(*Q) USER(FRED) AUT(*GET) MQMNAME(MYQMGR)
```

První dává oprávnění ke všem frontám pro činitele FRED s názvy, které odpovídají profilu AB. \*; druhý dává oprávnění ke stejným typům front, které odpovídají profilu AB.C\*.

Předpokládejme, že nyní vytvoříte frontu s názvem AB.CD. Podle pravidel pro shodu se zástupnými znaky může být GRTMQMAUT použit pro tuto frontu. Takže, má to dát nebo získat oprávnění?

Chcete-li najít odpověď, aplikujete pravidlo, které, kdykoli se může na objekt použít více profilů, **pouze nejspecifičtější použití**. Způsob použití tohoto pravidla je porovnáváním názvů profilů zleva doprava. Kdekoli se liší, negenerický znak je specifičtější než generický znak. Takže, v předchozím příkladu, fronta AB.CD má autoritu **get** (AB.C\* je více specifická než AB. \*).

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

1. ?
2. \*
3. \*\*

## Uvedení instalované autorizační služby na IBM i

Můžete uvést, která komponenta autorizační služby se má použít.

Parametr **Service Component name** na **GRTMQMAUT** a **RVKMQMAUT** vám umožňuje uvést název instalované komponenty autorizační služby.

Výběr volby **F24** na počátečním panelu, za nímž následuje příkaz **F9=All** na dalším panelu příkazu, umožňuje zadat buď instalovanou autorizační komponentu (\*DFT), nebo název požadované komponenty autorizační služby určené ve stanze Service v souboru qm.ini správce front.

**DSPMQMAUT** má také tento parametr navíc. Tento parametr vám umožňuje prohledat všechny nainstalované autorizační komponenty (\*DFT), nebo zadané jméno komponenty autorizační služby, pro uvedení názvu objektu, typ objektu a uživatele

## Práce s profily oprávnění a bez nich na serveru IBM i

V této části se dozvíte, jak pracovat s profily oprávnění a jak pracovat bez profilů oprávnění.

Můžete pracovat s profily oprávnění, jak je vysvětleno v publikaci [“Práce s profily oprávnění”](#) na stránce [168](#), nebo bez nich, jak je vysvětleno [zde](#):

Chcete-li pracovat bez profilů oprávnění, použijte \*NONE jako parametr oprávnění na **GRTMQMAUT**, abyste vytvořili profily bez oprávnění. To ponechá všechny existující profily nezměněné.

V systému **RVKMQMAUT** použijte jako parametr oprávnění \*REMOVE k odebrání existujícího profilu oprávnění.

## Práce s profily oprávnění

K profilování oprávnění jsou přidruženy dva příkazy:

- **WRKMQMAUT**
- **WRKMQMAUTD**

K těmto příkazům můžete přistoupit přímo z příkazového řádku nebo z panelu WRKMQM podle:

1. Zadání názvu správce front a stisknutí klávesy Enter pro přístup k panelu výsledků produktu **WRKMQM**.
2. Vyberte volbu F23=More options na tomto panelu.

Volba 24 vybere panel s výsledky pro příkaz **WRKMQMAUT** a volba 25 vybere příkaz **WRKMQMAUTI**, který se používá ve vrstvě vazeb SSL.

### WRKMQMAUT

Tento příkaz vám umožňuje pracovat s daty oprávnění zadrženými ve frontě oprávnění.

**Poznámka:** Chcete-li spustit tento příkaz, musíte mít oprávnění \*connect a \*admdsp ke správci front. Chcete-li však vytvořit nebo odstranit profil, potřebujete oprávnění QMQMADM.

Pokud tisknete informace na obrazovku, zobrazí se seznam názvů profilů oprávnění spolu s jejich typy. Pokud tisknete výstup, obdržíte podrobný seznam všech dat oprávnění, registrovaných uživatelů a jejich oprávnění.

Na tomto panelu zadejte název objektu nebo profilu a stisknutím klávesy Enter přejdete na panel výsledků pro produkt **WRKMQMAUT**.

Vyberete-li volbu 4=Delete, přejdete na nový panel, ze kterého můžete potvrdit, že chcete odstranit všechny názvy uživatelů zaregistrované na generický název profilu oprávnění, který jste zadali. Tato volba spustí **RVKMQMAUT** s volbou \*REMOVE pro všechny uživatele a použije **pouze** pro generické názvy profilů.

Vyberete-li volbu 12=Work with profile, přejdete na panel s výsledky příkazu **WRKMQMAUTD**, jak je vysvětleno v části "[WRKMQMAUTD](#)" na stránce 168.

### WRKMQMAUTD

Tento příkaz umožňuje zobrazit všechny uživatele registrované s určitým názvem profilu oprávnění a typem objektu. Chcete-li spustit tento příkaz, musíte mít oprávnění \*connect a \*admdsp ke správci front. Chcete-li však udělit, spustit, vytvořit nebo odstranit profil, který potřebujete, oprávnění QMQMADM.

Výběrem volby F24=More keys z počátečního vstupního panelu následovaným volbou F9=All Parameters se zobrazí název komponenty služby jako pro **GRTMQMAUT** a **RVKMQMAUT**.

**Poznámka:** Klávesa F11=Display Object Authorizations se přepíná mezi následujícími typy oprávnění:

- Oprávnění k objektu
- Kontextové autorizace
- Autorizace MQI

Volby na obrazovce jsou:

#### **2=Grant**

Vezme vás na panel **GRTMQMAUT**, abyste jej přidali do aktuálních oprávnění.

#### **3=Revoke**

Vezme vás na panel **RVKMQMAUT**, abyste odebrali některé z aktuálních definic

#### **4=Delete**

Přenesení vás na panel, který vám umožňuje odstranit data oprávnění pro uvedené uživatele. To spustí **RVKMQMAUT** s volbou \*REMOVE.

## 5=Display

Veźme vás na existující příkaz **DSPMQMAUT**

## F6=Create

Přenešete vás na panel **GRTMQMAUT** , který vám umožňuje vytvořit záznam oprávnění profilu.

## Pokyny správce oprávnění k objektu pro produkt IBM i

Další rady a tipy pro použití správce oprávnění k objektu (OAM)

### Omezit přístup k citlivým operacím

Některé operace jsou citlivé, omezují je na privilegované uživatele. Například

- Přístup k některým speciálním frontám, jako jsou přenosové fronty nebo fronta příkazů `SYSTEM . ADMIN . COMMAND . QUEUE`
- Spuštění programů, které používají úplné volby kontextu MQI
- Vytváření a kopírování front aplikací

### Adresáře správce front

Adresáře a knihovny obsahující fronty a další data správce front jsou pro daný produkt soukromé. Nepoužívejte standardní příkazy operačního systému k udělení nebo zrušení autorizace k prostředkům MQI.

### Fronty

Oprávnění k dynamické frontě je založené na, ale není nutně stejné jako u modelové fronty, ze které je odvozena.

Pro alias fronty a vzdálené fronty je to autorizace objektu samotného, ne fronty, na kterou je alias nebo vzdálená fronta vyřešena. Je možné autorizovat uživatelský profil pro přístup k frontě aliasů, která se překládá do lokální fronty, do které nemá uživatelský profil žádná přístupová oprávnění.

Omezte oprávnění k vytváření front pro privilegované uživatele. Pokud tak neuvidíte, uživatelé mohou obejít normální řízení přístupu vytvořením aliasu.

### Oprávnění alternativního uživatele

Oprávnění alternativního uživatele řídí, zda může jeden profil uživatele používat oprávnění jiného profilu uživatele při přístupu k objektu IBM MQ . Tato technika je nezbytná, pokud server přijímá požadavky od programu a server se chce 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.

Příklad:

- Serverový program spuštěný pod uživatelským profilem PAYSERV načte zprávu požadavku z fronty, která byla vložena do fronty profilem 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 místo použití vlastního profilu uživatele (PAYSERV) autorizovat otevření fronty pro odpovědi na frontu jiným uživatelským profilem, v tomto případě USER1. V tomto příkladu můžete použít alternativní oprávnění k řízení, zda má PAYSERV povoleno zadat USER1 jako alternativní profil uživatele při otevření fronty pro odpověď.

Profil alternativního uživatele je zadán v poli *AlternateUserId* v deskriptoru objektu.

**Poznámka:** Na libovolném objektu produktu IBM MQ můžete použít alternativní profily uživatele. Použití alternativního profilu uživatele nemá vliv na profil uživatele používaný jinými správci prostředků.

## Kontextové oprávnění

Kontext je informace, která se vztahuje ke konkrétní zprávě a která je obsažena v deskriptoru zpráv, MQMD, který je součástí zprávy.

Popisy polí deskriptoru zpráv týkajících se kontextu viz [Přehled MQMD](#).

Informace o volbách kontextu naleznete v tématu [Kontext zprávy](#).

## Aspekty vzdáleného zabezpečení

Pro vzdálené zabezpečení zvažte:

### Oprávnění pro operaci vložení (Put)

Pro zabezpečení ve všech správcích front můžete zadat oprávnění k vložení, které se použije v případě, že kanál přijme zprávu odeslanou z jiného správce front.

Tento parametr je platný pouze pro typy kanálů RCVR, RQSTR nebo CLUSRCVR. Specifikujte atribut kanálu PUTAUT následujícím způsobem:

#### DEF

Výchozí profil uživatele. Jedná se o profil uživatele QMQM, pod kterým je spuštěn agent kanálu zpráv.

#### CTX

Profil uživatele v kontextu zprávy.

### Přenosové fronty

Správci front automaticky umístí vzdálené zprávy do přenosové fronty; není vyžadováno žádné speciální oprávnění. Avšak vložení zprávy přímo do přenosové fronty vyžaduje speciální oprávnění.

### Uživatelské procedury kanálu

Uživatelské procedury kanálu lze použít pro přidání zabezpečení.

### Záznamy ověření kanálu

Používejte k větší přesné kontrole přístupu k připojovacím systémům na úrovni kanálu.

Další informace o vzdáleném zabezpečení viz [“Ověřování kanálu”](#) na stránce 95.

## Ochrana kanálů pomocí SSL nebo TLS

Protokoly SSL (Secure Sockets Layer) a TLS (Transport Layer Security) poskytují zabezpečení kanálu, s ochranou proti odposlouchávání, falšování a ztělesnění. Podpora produktu IBM MQ pro zabezpečení SSL a TLS vám umožňuje určit v definici kanálu, že konkrétní kanál používá zabezpečení SSL nebo TLS. Můžete také uvést podrobnosti o zabezpečení, které chcete, jako např. šifrovací algoritmus, který chcete použít.

Podpora zabezpečení SSL a TLS v produktu IBM MQ používá správce front *objekt ověřovacích informací* a různé příkazy CL a MQSC a správce front a parametry kanálu, které definují podporu zabezpečení SSL nebo TLS, jež jsou vyžadovány.

Následující příkazy CL podporují SSL nebo TLS:

#### WRKMQMAUTI

Práce s atributy objektu ověřovacích informací.

#### CHGMQMAUTI

Upravit atributy objektu ověřovacích informací.

#### CRMQMMUTIT

Vytvořte objekt ověřovacích informací.

#### CPYMQMAUTI

Vytvořte objekt ověřovacích informací zkopírováním existujícího objektu.

#### DLMQMAUTI

Odstraňte objekt ověřovacích informací.

## DSPMQMAUTI

Zobrazí atributy pro specifický objekt ověřovacích informací.

Přehled zabezpečení kanálu s použitím zabezpečení SSL nebo protokolu TLS naleznete v tématu

- [Ochrana kanálů pomocí SSL](#)

Podrobnosti o příkazech PCF přidružených k SSL viz

- [Změnit, kopírovat a vytvořit objekt ověřovacích informací](#)
- [Odstranit objekt ověřovacích informací](#)
- [Dotaz na objekt ověřovacích informací](#)

## Nastavení zabezpečení v systému z/OS

Aspekty zabezpečení specifické pro produkt z/OS.

Zabezpečení v produktu IBM MQ for z/OS je řízeno pomocí produktu RACF nebo ekvivalentního externího správce zabezpečení (ESM).

Má-li ID uživatele uid0, má přístup k celému systému souborů, to jest k přístupu superuživatele. V části RACF je jediným způsobem, jak toto omezení omezit, použití funkce FSACCESS, která omezuje přístup na úrovni systému souborů pomocí ID uživatele produktu RACF. Další informace naleznete v tématu [Použití profilu třídy FSDACCESS k omezení přístupu](#) v dokumentaci produktu *z/OS UNIX System Services Planning*.

Následující pokyny předpokládají, že používáte produkt RACF.

### Související informace

[Scénář zabezpečení: dva správci front v systému z/OS](#)

[Scénář zabezpečení: skupina sdílení front v systému z/OS](#)

## Třídy zabezpečení produktu RACF

Třídy RACF se používají k uchování profilů požadovaných pro kontrolu zabezpečení produktu IBM MQ. Řada z tříd členů má ekvivalentní třídy skupin. Musíte aktivovat třídy a povolit jim přijetí generických profilů

Každá třída RACF obsahuje jeden nebo více profilů použitých v určitém bodě v kontrolní posloupnosti, jak je zobrazeno v části [Tabulka 23 na stránce 171](#).

<b>Třída členů</b>	<b>Třída skupiny</b>	<b>Obsah</b>
MQADMIN	GMQADMIN	Profily: Používají se hlavně pro držení profilů pro funkce administrativního typu. Příklad: <ul style="list-style-type: none"><li>• Profily pro přepínače zabezpečení produktu IBM MQ</li><li>• Profil zabezpečení RESLEVEL</li><li>• Profily pro alternativní zabezpečení uživatelů</li><li>• Profil kontextu zabezpečení</li><li>• Profily pro zabezpečení prostředků příkazů</li></ul>



Tabulka 23. Třídy RACF použité produktem IBM MQ (pokračování)

Třída členů	Třída skupiny	Obsah
MXADMIN	GMXADMIN	<p>Profily:</p> <p>Používají se hlavně pro držení profilů pro funkce administrativního typu. Příklad:</p> <ul style="list-style-type: none"> <li>• Profily pro přepínače zabezpečení produktu IBM MQ</li> <li>• Profil zabezpečení RESLEVEL</li> <li>• Profily pro alternativní zabezpečení uživatelů</li> <li>• Profil kontextu zabezpečení</li> <li>• Profily pro zabezpečení prostředků příkazů</li> </ul> <p>Tato třída může obsahovat velké i velké profily produktu RACF s velkými i malými písmeny.</p>
MQCONN		Profily použité pro zabezpečení připojení
MQCMD5		Profily použité pro zabezpečení příkazů
MQQUEUE	FRONTA GMQUEUE	Profily použité ve zabezpečení prostředků fronty
MXQUEUE	GMXQUEUE	Kombinované profily velkých a malých písmen použité ve zabezpečení prostředků fronty
MQPROC	GMQPROC	Profily použité v zabezpečení prostředků procesu
MXPROC	GMXPROC	Kombinované profily velkých a malých písmen použité v zabezpečení prostředků procesu
MQNLIST	SEZNAM GMQNLIST	Profily použité v zabezpečení prostředků seznamu názvů
MXNLIST	GMXNLIST	Smíšený případ a profily velkých písmen použité v zabezpečení prostředků seznamu názvů
MXTOPIC	GMXTOPIC	Kombinované profily velkých a malých písmen použité v zabezpečení témat

Některé třídy mají související *třidu skupiny*, která vám umožňuje dát dohromady skupiny prostředků s podobnými požadavky na přístup. Podrobnosti o rozdílu mezi členskou a skupinovou třídou a při použití členu nebo třídy skupiny naleznete v příručce *z/OS Security Server RACF Security Administrator's Guide*.

Třídy musí být aktivovány před tím, než mohou být provedeny kontroly zabezpečení. Chcete-li aktivovat všechny třídy IBM MQ, můžete použít tento příkaz RACF :

```
SETROPTS CLASSACT(MQADMIN, MXADMIN, MQQUEUE, MXQUEUE, MQPROC, MXPROC,
MQNLIST, MXNLIST, MXTOPIC, MQCONN, MQCMD5)
```

Měli byste také zajistit, abyste nastavili třídy tak, aby mohly přijímat generické profily. Toto provedete také pomocí příkazu RACF SETROPTS, například:

```
SETROPTS GENERIC(MQADMIN, MXADMIN, MQQUEUE, MXQUEUE, MQPROC, MXPROC,
MQNLIST, MXNLIST, MXTOPIC, MQCONN, MQCMD5)
```

## RACF profily

Všechny profily produktu RACF používané produktem IBM MQ obsahují předponu, což je buď název správce front, nebo název skupiny sdílení front. Při použití znaku procenta jako zástupného znaku buďte opatrní.

Všechny profily produktu RACF použité produktem IBM MQ obsahují předponu. Pro zabezpečení na úrovni skupiny sdílení front se jedná o název skupiny sdílení front. Pro úroveň zabezpečení správce front je předponou název správce front. Používáte-li směs správce front a zabezpečení na úrovni skupiny sdílení front, budete používat profily s oběma typy předpon. (Skupina sdílení front a zabezpečení na úrovni správce front jsou popsány v tématu [Koncepce produktu IBM MQ for z/OS : Zabezpečení](#).)

Chcete-li například chránit frontu s názvem `QUEUE_FOR_SUBSCRIBER_LIST` ve skupině sdílení front `QSG1` na úrovni skupiny sdílení front, bude vhodný profil definován jako RACF jako:

```
RDEFINE MQQUEUE QSG1.QUEUE_FOR_SUBSCRIBER_LIST
```

Chcete-li chránit frontu s názvem `QUEUE_FOR_LOST_CARD_LIST`, která náleží do správce front `STCD` na úrovni správce front, bude příslušný profil definován jako RACF jako:

```
RDEFINE MQQUEUE STCD.QUEUE_FOR_LOST_CARD_LIST
```

To znamená, že různí správci front a skupiny sdílení front mohou sdílet stejnou databázi RACF a mít však jiné volby zabezpečení.

Nepoužívejte generické názvy správce front v profilech, abyste se vyhnuli nepředpokládanému přístupu uživatelů.

IBM MQ umožňuje použití znaku procenta (%) v názvech objektů. RACF však používá znak% jako zástupný znak s jedním znakem. To znamená, že když definujete jméno objektu se znakem% v jeho názvu, musíte to vzít v úvahu při definování odpovídajícího profilu.

For example, for the queue `CREDIT_CARD_%_RATE_INQUIRY`, on queue manager `CRDP`, the profile would be defined to RACF as follows:

```
RDEFINE MQQUEUE CRDP.CREDIT_CARD_%_RATE_INQUIRY
```

Tuto frontu nelze chránit generickým profilem, jako např. `CRDP.*`.

IBM MQ umožňuje použití smíšených znaků velkých a malých písmen v názvech objektů. Tyto objekty můžete chránit definováním:

1. Kombinované profily případu v příslušných třídách RACF se smíšenými velkými i malými písmeny, nebo
2. Generické profily v příslušných velkých třídách RACF .

Chcete-li použít kombinaci profilů velkých a malých písmen a smíšených tříd produktu RACF , musíte postupovat podle kroků popsaných v tématu [z/OS Migrace správce front na zabezpečení se smíšenými malými a velkými písmeny](#).

Jsou zde některé profily nebo části profilů, které zůstávají velkými písmeny pouze v případě, že jsou hodnoty poskytnuty produktem IBM MQ. Patří mezi ně:

- Přepnout profily.
- Všechny kvalifikátory vysoké úrovně (HLQ) včetně identifikátorů skupin subsystémů a front-sdílení front.
- Profily pro objekty `SYSTEM`.
- Profily pro výchozí objekty.
- Třída **MQCMDS** , takže všechny profily příkazů jsou pouze velká písmena.
- Třída **MQCONN** , takže všechny profily připojení jsou pouze velká písmena.

- Profily produktu **RESLEVEL** .
- Kvalifikace produktu 'object' v profilech prostředků příkazu; například hlq.QUEUE.queueName. Název prostředku je pouze malá a velká písmena.
- Dynamické profily front hlq.CSQOREXX.\* , hlq.CSQUTIL.\*a CSQXCMD.\*.
- 'CONTEXT' části produktu hlq.CONTEXT.resourcename.
- Část 'ALTERNATE.USER' části hlq.ALTERNATE.USER.userid.

Máte-li například frontu s názvem PAYROLL.Dept1 ve správci front QM01 a používáte-li:

- Smíšené profily případu; můžete definovat profil ve třídě IBM MQ RACF MXQUEUE

```
RDEFINE MXQUEUE MQ01.PAYROLL.Dept1
```

- Velké profily; můžete definovat profil ve třídě IBM MQ RACF MQQUEUE

```
RDEFINE MQQUEUE MQ01.PAYROLL.*
```

První příklad použití smíšených profilů malých a velkých písmen vám dává přesnější kontrolu nad udělením oprávnění pro přístup k prostředku.

## Profily přepínače

Chcete-li řídit kontrolu zabezpečení provedenou produktem IBM MQ, použijte *profily přepínače*. Profil přepínače je normální profil RACF , který má speciální význam pro IBM MQ. Seznam pro přístup v profilech přepínačů není používán produktem IBM MQ.

Produkt IBM MQ udržuje interní přepínač pro každý typ přepínače zobrazený v tabulkách [Přepnout profily pro zabezpečení na úrovni subsystému](#), [Profily přepínače pro skupinu sdílení front nebo zabezpečení na úrovni správce fronta](#) [Přepnout profily pro kontrolu prostředků](#). Profily přepínače lze udržovat na úrovni skupiny sdílení front, nebo na úrovni správce front nebo v kombinaci obou. Pomocí jediné sady profilů přepínače zabezpečení skupiny sdílení front můžete řídit zabezpečení všech správců front v rámci skupiny sdílení front.

Je-li nastaven přepínač zabezpečení, provedou se kontroly zabezpečení přidružené k přepínači. Je-li přepínač zabezpečení vypnut, bezpečnostní kontroly přidružené k přepínači budou vynechány. Předvolba je, že jsou nastaveny všechny přepínače zabezpečení.

## Přepínače a třídy

Když spustíte správce front nebo aktualizujete zabezpečení, produkt IBM MQ nastaví přepínače podle stavu různých tříd produktu RACF .

Když je správce front spuštěn (nebo když je třída MQADMIN nebo MXADMIN obnovena příkazem IBM MQ [REFRESH SECURITY](#) ), produkt IBM MQ nejprve zkontroluje stav RACF a příslušné třídy:

- Třída MQADMIN, používáte-li velké profily
- Třída MXADMIN, používáte-li smíšený profil případu.

Je-li některá z těchto podmínek pravdivá, nastaví přepínač zabezpečení subsystému:

- RACF je neaktivní nebo není instalovaný.
- Třída MQADMIN nebo MXADMIN není definována (tyto třídy jsou vždy definovány pro RACF , protože jsou zahrnuty v tabulce deskriptorů třídy (CDT)).
- Třída MQADMIN nebo MXADMIN nebyla aktivována.

Je-li třída RACF i třída MQADMIN nebo MXADMIN aktivní, produkt IBM MQ zkontroluje třídu MQADMIN nebo MXADMIN, aby zjistil, zda některý z profilů přepínačů nebyl definován. Nejprve zkontroluje profily popsané v části “[Profily pro řízení zabezpečení subsystému](#)” na stránce 175. Není-li zabezpečení subsystému vyžadováno, IBM MQ nastaví zabezpečení interního subsystému a neprovede žádné další kontroly.

Profily určují, zda je odpovídající přepínač IBM MQ zapnutý nebo vypnutý.

- Je-li přepínač vypnutý, je tento typ zabezpečení deaktivován.
- Je-li nastaven některý z přepínačů IBM MQ , program IBM MQ zkontroluje stav třídy RACF přidružené k typu zabezpečení, který odpovídá přepínači IBM MQ . Není-li třída nainstalována nebo není aktivní, je přepínač IBM MQ vypnut. Kontroly zabezpečení procesů se například neprovádějí, pokud nebyla aktivována třída MQPROC nebo MXPROC. Třída, která není aktivní, je ekvivalentní definování NO.PROCESS.CHECKS profil pro každého správce front a skupinu sdílení front, která používá tuto databázi RACF .

### **Jak fungují přepínače**

Chcete-li nastavit přepínač zabezpečení, definujte hodnotu NO.\*. Profil přepínače pro tento profil. NOV.\* lze přepsat. profil nastavený na úrovni skupiny sdílení front definováním YES.\* pro správce front.

Chcete-li nastavit přepínač zabezpečení, je třeba definovat hodnotu NO.\*. Profil přepínače pro tento profil. Existence položky NO.\* profil znamená, že kontroly zabezpečení **nejsou** prováděny pro daný typ prostředku, pokud se nerozhodnete přepsat nastavení úrovně skupiny sdílení front v konkrétním správci front. Tento popis je popsán v tématu [“Potlačení nastavení úrovně skupiny sdílení front”](#) na stránce 175.

Pokud váš správce front není členem skupiny sdílení front, není třeba definovat žádné profily úrovně skupiny sdílení front ani žádné profily potlačení. Je však třeba tyto profily definovat, pokud se správce front připojí ke skupině sdílení front k pozdějšímu datu.

Každý NO.\* Profil přepínače, který příkaz IBM MQ detekuje, vypíná kontrolu daného typu prostředku. Profily přepnutí se aktivují při spuštění správce front. Pokud změníte profily přepínače, zatímco jsou spuštěni všichni postižení správci front, můžete produkt IBM MQ získat, aby rozpoznal změny vydáním příkazu IBM MQ REFRESH SECURITY.

Profily přepínače musí být vždy definovány ve třídě MQADMIN nebo MXADMIN. Nedefinujte je ve třídě GMQADMIN nebo GMXADMIN. Tabulky [Přepnout profily pro zabezpečení na úrovni subsystému](#) a [Přepnutí profilů pro kontrolu prostředků](#) zobrazují platné profily přepínače a typ zabezpečení, který řídí.

### **Potlačení nastavení úrovně skupiny sdílení front**

Nastavení zabezpečení na úrovni skupiny sdílení front pro konkrétního správce front, který je členem této skupiny, lze přepsat. Chcete-li provést kontroly správce front v jednotlivých správcích front, které nejsou provedeny v jiných správcích front ve skupině, použijte příkaz (qmgr-name.YES. \*) profily přepínačů.

Naopak, pokud nechcete provést určitou kontrolu u jednoho konkrétního správce front v rámci skupiny sdílení front, definujte soubor (qmgr-name.NO. \*) profilu pro tento konkrétní typ prostředku ve správci front a nedefinujte profil pro skupinu sdílení front. ( IBM MQ kontroluje pouze profil úrovně skupiny sdílení front, pokud nenajde profil úrovně správce front.)

### **Profily pro řízení zabezpečení subsystému**

Produkt IBM MQ kontroluje, zda jsou pro subsystém, pro správce front a pro skupinu sdílení front vyžadovány kontroly zabezpečení subsystému.

První kontrola zabezpečení provedená pomocí IBM MQ se používá k určení, zda jsou bezpečnostní kontroly vyžadovány pro celý subsystém IBM MQ . Pokud uvedete, že nechcete zabezpečení subsystému, nebudou provedeny žádné další kontroly.

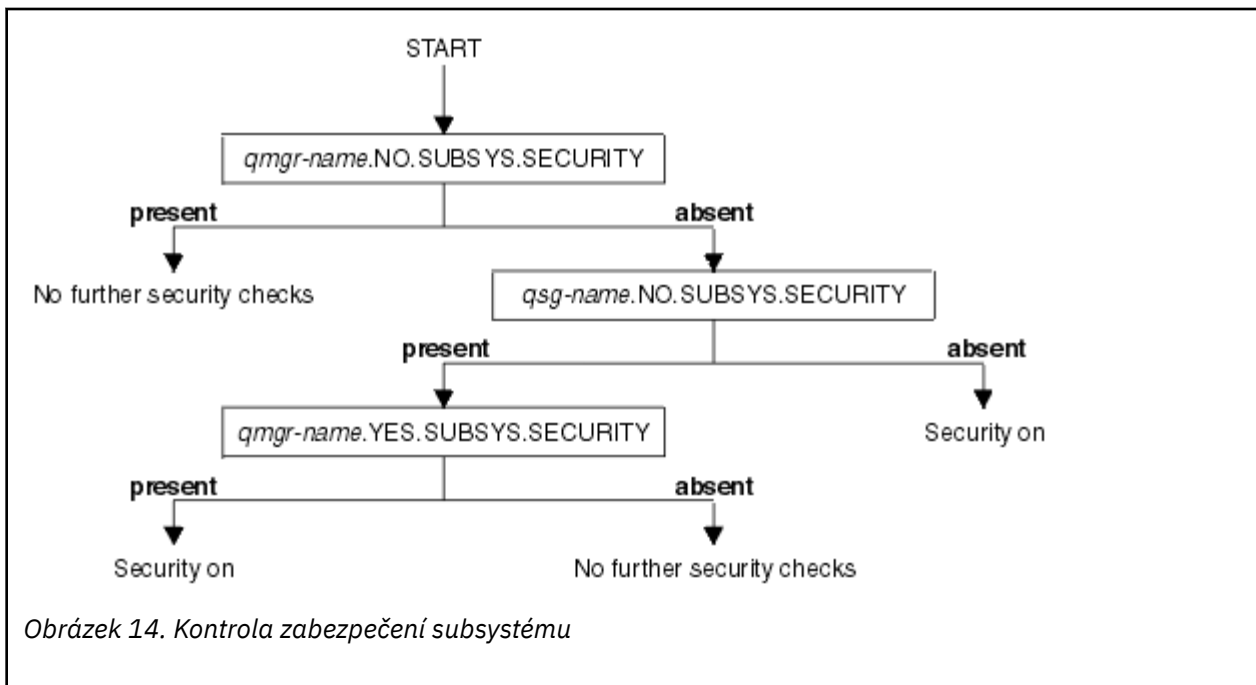
Jsou zkontrolovány následující profily přepínače, aby se určilo, zda je zabezpečení subsystému povinné. [Obrázek 14](#) na stránce 176 zobrazuje pořadí, ve kterém jsou zkontrolovány.

Název profilu přepínače	Typ prostředku nebo kontrolování, které je řízeno
qmgr-name.NO.SUBSYS.SECURITY	Zabezpečení podsystému pro tohoto správce front
qsg-name.NO.SUBSYS.SECURITY	Zabezpečení subsystému pro tuto skupinu sdílení front

Tabulka 24. Přepnout profily pro zabezpečení na úrovni subsystému (pokračování)

Název profilu přepínače	Typ prostředku nebo kontrolování, které je řízeno
qmgr-name.YES.SUBSYS.SECURITY	Potlačení zabezpečení subsystému pro tohoto správce front

Pokud váš správce front není členem skupiny sdílení front, příkaz IBM MQ vyhledá pouze profil přepínače qmgr-name.NO.SUBSYS.SECURITY .



### Profily pro řízení zabezpečení na úrovni skupiny sdílení front nebo správce front

Je-li kontrola zabezpečení subsystému vyžadována, produkt IBM MQ kontroluje, zda je kontrola zabezpečení vyžadována ve skupině sdílení front nebo na úrovni správce front.

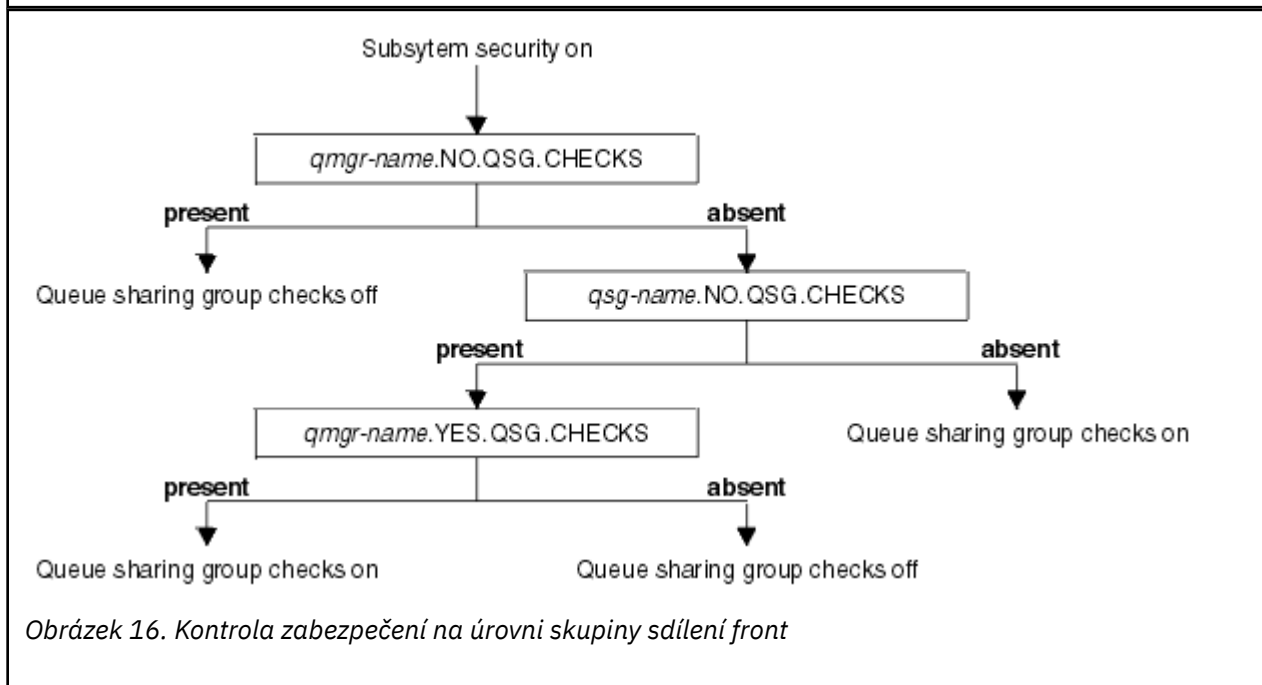
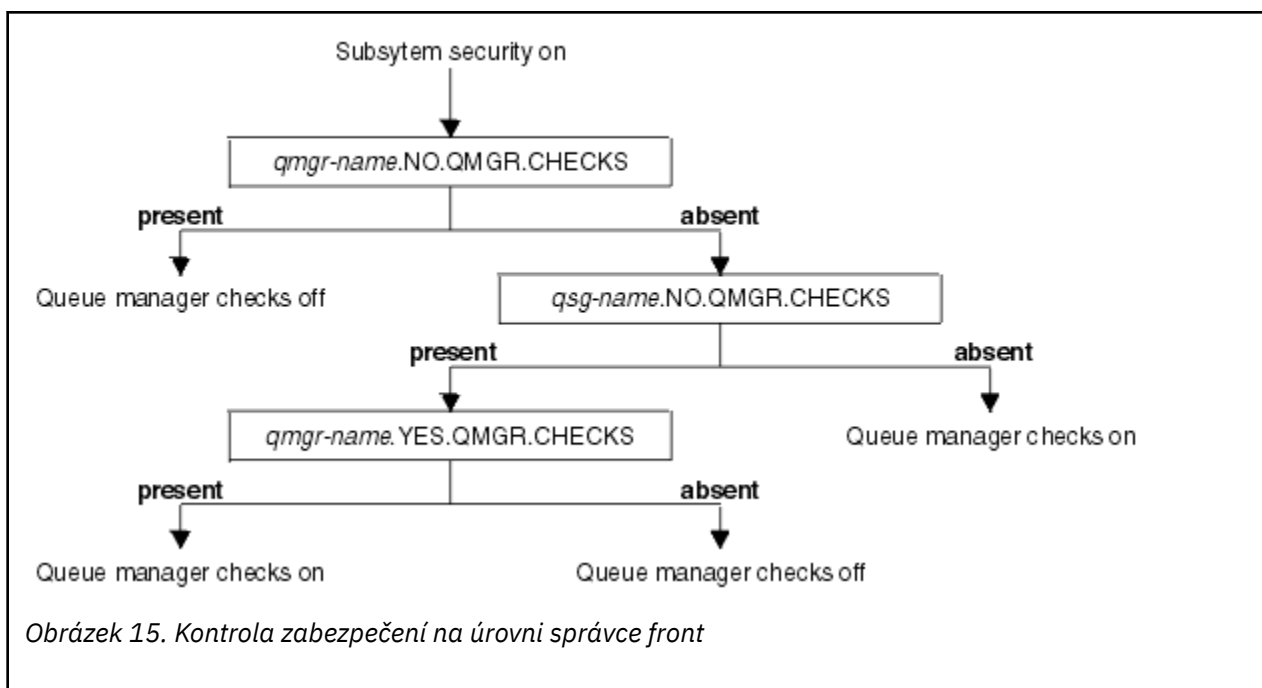
Když produkt IBM MQ určil, že je vyžadována kontrola zabezpečení, pak určuje, zda je vyžadována kontrola na úrovni skupiny sdílení front nebo správce front, nebo obojí. Tyto kontroly se neprovedou, pokud váš správce front není členem skupiny sdílení front.

Požadují se následující profily přepínačů, aby bylo možné určit požadovanou úroveň. Obrázek 15 na stránce 177 a Obrázek 16 na stránce 177 zobrazují pořadí, ve kterém jsou zaškrtnuty.

Tabulka 25. Přepnout profily pro skupinu sdílení front nebo zabezpečení na úrovni správce front

Název profilu přepínače	Typ prostředku nebo kontrolování, které je řízeno
qmgr-name.NO.QMGR.CHECKS	Žádné kontroly úrovně správce front pro tohoto správce front
qsg-name.NO.QMGR.CHECKS	Pro tuto skupinu sdílení front nejsou žádné kontroly na úrovni správce front.
qmgr-name.YES.QMGR.CHECKS	Přepsání kontroly úrovně správce front pro tohoto správce front
qmgr-name.NO.QSG.CHECKS	Žádné kontroly úrovně skupiny sdílení front pro tohoto správce front
qsg-name.NO.QSG.CHECKS	Pro tuto skupinu sdílení front neexistují žádné kontroly úrovně skupiny sdílení front
qmgr-name.YES.QSG.CHECKS	Přepis nastavení kontroly úrovně skupiny sdílení front pro tohoto správce front

Je-li zabezpečení subsystému aktivní, nemůžete vypnout jak skupinu sdílení front, tak zabezpečení na úrovni správce front. Pokud se o to pokusíte, produkt IBM MQ nastaví kontrolu zabezpečení na obou úrovních.



*Platné kombinace přepínačů zabezpečení*

Platné jsou pouze některé kombinace přepínačů. Pokud použijete kombinaci nastavení přepínačů, která není platná, je vydána zpráva CSQH026I a kontrola zabezpečení je nastavena na úrovni skupiny sdílení front i na úrovni správce front.

Tabulka 26 na stránce 178, Tabulka 27 na stránce 178, Tabulka 28 na stránce 178a Tabulka 29 na stránce 179 zobrazují sady kombinací nastavení přepínačů, které jsou platné pro každý typ úrovně zabezpečení.

*Tabulka 26. Platné kombinace přepínačů zabezpečení pro zabezpečení na úrovni správce front*

<b>Kombinace</b>
qmgr-name.NO.QSG.CHECKS
qsg-name.NO.QSG.CHECKS
qmgr-name.NO.QSG.CHECKS qsg-name.NO.QMGR.CHECKS qmgr-name.YES.QMGR.CHECKS
qsg-name.NO.QSG.CHECKS qsg-name.NO.QMGR.CHECKS qmgr-name.YES.QMGR.CHECKS

*Tabulka 27. Platné kombinace přepínačů zabezpečení pro zabezpečení na úrovni skupiny sdílení front*

<b>Kombinace</b>
qmgr-name.NO.QMGR.CHECKS
qsg-name.NO.QMGR.CHECKS
qmgr-name.NO.QMGR.CHECKS qsg-name.NO.QSG.CHECKS qmgr-name.YES.QSG.CHECKS
qsg-name.NO.QMGR.CHECKS qsg-name.NO.QSG.CHECKS qmgr-name.YES.QSG.CHECKS

*Tabulka 28. Platné kombinace přepínačů zabezpečení pro správce front a zabezpečení na úrovni skupiny sdílení front*

<b>Kombinace</b>
qsg-name.NO.QMGR.CHECKS qmgr-name.YES.QMGR.CHECKS Ne QSG.* definované profily
Žádný QMGR.* definované profily qsg-name.NO.QSG.CHECKS qmgr-name.YES.QSG.CHECKS
qsg-name.NO.QMGR.CHECKS qmgr-name.YES.QMGR.CHECKS qsg-name.NO.QSG.CHECKS qmgr-name.YES.QSG.CHECKS
Nejsou definovány žádné profily pro definovaný přepínač

Tabulka 29. Další platné kombinace přepínačů zabezpečení, které přepínají obě úrovně kontroly **zapnu**.

<b>Kombinace</b>
qmgr-name.NO.QMGR.CHECKS qmgr-name.NO.QSG.CHECKS
qsg-name.NO.QMGR.CHECKS qsg-name.NO.QSG.CHECKS
qmgr-name.NO.QMGR.CHECKS qsg-name.NO.QSG.CHECKS
qsg-name.NO.QMGR.CHECKS qmgr-name.NO.QSG.CHECKS

### Kontroly na úrovni prostředků

K řízení přístupu k prostředkům se používá řada profilů přepínačů. Některé kontroly ukončení jsou prováděny buď ve správci front, nebo ve skupině sdílení front. Ty mohou být přepsány profily, které umožňují kontrolu pro specifické správce front.

Tabulka 30 na stránce 179 zobrazuje profily přepínače používané k řízení přístupu k prostředkům produktu IBM MQ .

Je-li váš správce front součástí skupiny sdílení front a máte-li aktivní zabezpečení skupiny správců front i skupiny sdílení front, můžete použít prvek YES.\* profil přepínače potlačí profily úrovně skupiny sdílení front a konkrétně zapne zabezpečení pro určitého správce front.

Některé profily se vztahují na správce front i skupiny sdílení front. Tyto řetězce jsou označeny řetězcem *hlq* a vy byste měli nahradit název vaší skupiny sdílení front nebo správce front, jak je relevantní. Názvy profilů s předponou *qmgr-name* jsou přepisující profily správce front; měli byste nahradit název správce front.

Tabulka 30. Přepnout profily pro kontrolu prostředků

Typ kontroly prostředků, která je řízena	Název profilu přepínače	Přepsat profil pro určitého správce front
Zabezpečení připojení	hlq.NO.CONNECT.CHECKS	qmgr-name.YES.CONNECT.CHECKS
Zabezpečení fronty	hlq.NO.QUEUE.CHECKS	qmgr-name.YES.QUEUE.CHECKS
Zabezpečení procesu	hlq.NO.PROCESS.CHECKS	qmgr-name.YES.PROCESS.CHECKS
Zabezpečení seznamu názvů	hlq.NO.NLIST.CHECKS	qmgr-name.YES.NLIST.CHECKS
zabezpečení kontextu	hlq.NO.CONTEXT.CHECKS	qmgr-name.YES.CONTEXT.CHECKS
alternativní zabezpečení uživatele	hlq.NO.ALTERNATE.USER.CHECKS	qmgr-name.YES.ALTERNATE.USER.CHECKS
Zabezpečení příkazů	hlq.NO.CMD.CHECKS	qmgr-name.YES.CMD.CHECKS
Zabezpečení prostředků příkazů	hlq.NO.CMD.RESC.CHECKS	qmgr-name.YES.CMD.RESC.CHECKS



Tabulka 30. Přepnout profily pro kontrolu prostředků (pokračování)

Typ kontroly prostředků, která je řízena	Název profilu přepínače	Přepsat profil pro určitého správce front
Zabezpečení tématu	hlq.NO.TOPIC.CHECKS	qmgr-name.YES.TOPIC.CHECKS
<b>Poznámka:</b> Generické profily přepínače, jako například hlq.NO. * * jsou ignorovány IBM MQ		

Chcete-li například provést kontroly zabezpečení procesu ve správci front QM01, který je členem skupiny sdílení front QSG3, ale nechcete provést kontroly zabezpečení procesu u žádného z ostatních správců front ve skupině, definujte následující profily přepínače:

```
QSG3.NO.PROCESS.CHECKS
QM01.YES.PROCESS.CHECKS
```

Chcete-li provést kontroly zabezpečení fronty prováděné u všech správců front ve skupině sdílení front, s výjimkou QM02, definujte následující profil přepínače:

```
QM02.NO.QUEUE.CHECKS
```

(Pro skupinu sdílení front není třeba definovat profil, protože kontroly jsou automaticky povoleny, pokud není definován žádný profil.)

### **Příklad definování přepínačů**

Různé subsystémy IBM MQ mají různé požadavky na zabezpečení, které lze implementovat pomocí různých profilů přepínačů.

Byly definovány čtyři subsystémy IBM MQ :

- MQP1 (produkční systém)
- MQP2 (produkční systém)
- MQD1 (vývojový systém)
- MQT1 (testovací systém)

Všichni čtyři správci front jsou členy skupiny sdílení front QS01. Všechny třídy produktu IBM MQ RACF byly definovány a aktivovány.

Tyto subsystémy mají různé požadavky na zabezpečení:

- Produkční systémy vyžadují plnou kontrolu zabezpečení produktu IBM MQ na úrovni skupiny sdílení front v obou systémech.

To se provádí zadáním následujícího profilu:

```
RDEFINE MQADMIN QS01.NO.QMGR.CHECKS
```

Tato hodnota nastavuje kontrolu úrovně skupiny sdílení front pro všechny správce front v rámci skupiny sdílení front. Pro provozní správce front nemusíte definovat žádné jiné profily přepínačů, protože chcete zkontrolovat vše pro tyto systémy.

- Při testu správce front MQT1 je vyžadována také úplná kontrola zabezpečení. Vzhledem k tomu, že je však vhodné později změnit, lze zabezpečení definovat na úrovni správce front, abyste mohli změnit nastavení zabezpečení pro tohoto správce front, aniž by to mělo vliv na ostatní členy skupiny sdílení front.

To provedete tak, že definujete NO.QSG.CHECKS profil pro MQT1 následujícím způsobem:

```
RDEFINE MQADMIN MQT1.NO.QSG.CHECKS
```

- Správce front vývoje MQD1 má odlišné požadavky na zabezpečení od zbytku skupiny sdílení front. Vyžaduje to pouze připojení a zabezpečení fronty, aby bylo aktivní.

To lze provést definováním profilu produktu MQD1 . YES . QMGR . CHECKS pro tohoto správce front a následným definováním následujících profilů pro vypnutí kontroly zabezpečení pro prostředky, které není třeba zkontrolovat:

```
RDEFINE MQADMIN MQD1.NO.CMD.CHECKS
RDEFINE MQADMIN MQD1.NO.CMD.RESC.CHECKS
RDEFINE MQADMIN MQD1.NO.PROCESS.CHECKS
RDEFINE MQADMIN MQD1.NO.NLIST.CHECKS
RDEFINE MQADMIN MQD1.NO.CONTEXT.CHECKS
RDEFINE MQADMIN MQD1.NO.ALTERNATE.USER.CHECKS
```

Je-li správce front aktivní, můžete zobrazit aktuální nastavení zabezpečení zadáním příkazu DISPLAY SECURITY MQSC.

Nastavení přepínače můžete změnit také tehdy, je-li správce front spuštěn definováním nebo odstraněním příslušného profilu přepínače ve třídě MQADMIN. Chcete-li, aby změny nastavení přepínače byly aktivní, je třeba pro třídu MQADMIN zadat příkaz REFRESH SECURITY.

Další informace o použití příkazů DISPLAY SECURITY a REFRESH SECURITY naleznete v příručce [“Aktualizace zabezpečení správce front v systému z/OS”](#) na stránce 233 .

## Profily používané k řízení přístupu k prostředkům produktu IBM MQ

Chcete-li řídit přístup k prostředkům produktu IBM MQ , musíte kromě profilů přepínačů, které mohly být definovány, definovat profily produktu RACF . Tato kolekce témat obsahuje informace o profilech produktu RACF pro různé typy prostředků produktu IBM MQ .

Pokud nemáte definován profil prostředku pro konkrétní kontrolu zabezpečení a uživatel vydá požadavek, který by zahrnoval provedení této kontroly, příkaz IBM MQ odepřel přístup. Nemusíte definovat profily pro typy zabezpečení vztahující se k žádným přepínačům zabezpečení, které jste deaktivovali.

### **Profily pro zabezpečení připojení**

Je-li zabezpečení připojení aktivní, je třeba definovat profily ve třídě MQCONN a povolit k těmto profilům přístup nezbytné skupiny nebo ID uživatelů, aby se mohly připojit k produktu IBM MQ.

Chcete-li povolit vytvoření připojení, musíte uživatelům produktu RACF READ udělit přístup k příslušnému profilu. (Pokud neexistuje žádný profil úrovně správce front a váš správce front je členem skupiny sdílení front, mohou být provedeny kontroly vzhledem k profilům na úrovni skupiny sdílení front, je-li zabezpečení nastaveno tak, aby bylo toto provedeno.)

Profil připojení s názvem správce front řídí přístup ke specifickému správci front a uživatelé s přístupem k tomuto profilu se mohou připojit k danému správci front. Profil připojení kvalifikovaný s názvem skupiny sdílení front řídí přístup ke všem správcům front v rámci skupiny sdílení front pro daný typ připojení. Uživatel s přístupem k produktu QS01 . BATCH může například používat dávkové připojení k libovolnému správci front ve skupině sdílení front QS01 , který nemá definován profil úrovně správce front.

### **Poznámka:**

1. Informace o ID uživatelů zkontrolovaných pro různé požadavky na zabezpečení najdete v tématu [“ID uživatele pro kontrolu zabezpečení”](#) na stránce 222.
2. Kontroly úrovně zabezpečení na úrovni prostředku (RESLEVEL) jsou také prováděny v době připojení. Podrobnosti viz část [“Profil zabezpečení RESLEVEL”](#) na stránce 217.

Zabezpečení produktu IBM MQ rozpoznává následující různé typy připojení:

- Mezi připojeními typu dávka (a dávkového typu) patří následující:
  - z/OS Dávkové úlohy
  - Aplikace TSO
  - Přihlášení USS

- Db2Uložené procedury
- CICS připojení
- IMS připojení z řídicích a aplikačních oblastí zpracování
- Inicializátor kanálu IBM MQ

#### *Profily zabezpečení připojení pro dávkové připojení*

Profily pro kontrolu spojení typu dávky se skládají z názvu správce front nebo názvu skupiny sdílení front následovaného slovem *BATCH*. Poskytněte ID uživatele přidružené k připojenému adresnímu prostoru READ přístup k profilu připojení.

Profily pro kontrolu dávkových a dávkových typů připojení mají tento tvar:

```
h1q.BATCH
```

kde *h1q* může být buď *qmgr-name* (název správce front), nebo *qsg-name* (název skupiny sdílení front). Používáte-li správce front i zabezpečení na úrovni skupiny sdílení front, produkt IBM MQ vyhledá profil s předponou názvu správce front. Pokud ji nenajde, hledá profil s předponou název skupiny sdílení front. Pokud se nepodaří najít žádný profil, požadavek na připojení selže.

Pro dávkové nebo dávkové požadavky na připojení musíte povolit ID uživatele přidruženého k připojenému adresnímu prostoru pro přístup k profilu připojení. Například následující příkaz RACF umožňuje uživatelům ve skupině CONNTQM1 připojit se ke správci front TQM1; těchto ID uživatelů bude povoleno používat dávkové připojení nebo připojení dávkového typu.

```
RDEFINE MQCONN TQM1.BATCH UACC(NONE)
PERMIT TQM1.BATCH CLASS(MQCONN) ID(CONNTQM1) ACCESS(READ)
```

#### *Použití produktu **CHCKLOCL** v lokálně vázaných aplikacích*

**CHCKLOCL** se vztahuje pouze na spojení, která jsou prováděna přes připojení BATCH a nevztahuje se na spojení vyrobená z produktů CICS nebo IMS. Připojení provedená prostřednictvím inicializátoru kanálu jsou řízena produktem **CHCKCLNT**.

## Přehled

Chcete-li nakonfigurovat správce front produktu z/OS tak, aby kontroloval ID uživatele a kontrolu hesla pro některé, ale ne všechny lokálně vázané aplikace, je třeba provést další konfiguraci.

Důvodem pro toto je, že jakmile je nakonfigurováno **CHCKLOCL** (*REQUIRED*), starší dávkové aplikace, které používají volání rozhraní API MQCONN, se již nemohou připojovat ke správci front.

Pouze pro systém z/OS lze použít k downgrade globální konfigurace **CHCKLOCL** (*REQUIRED*) do **CHCKLOCL** (*VOLITELNÉ*) pro specificky definovaná ID uživatele granulární mechanismus založený na zabezpečení připojení adresního prostoru. Použitý mechanismus je popsán v následujícím textu společně s příkladem.

Chcete-li povolit větší granularitu na **CHCKLOCL** (*REQUIRED*) než pouze *EVERYONE*, upravíte **CHCKLOCL** stejným způsobem, jak upravíte úroveň přístupu ID uživatele přidruženého k připojenému adresnímu prostoru k profilům připojení *h1q.batch* ve třídě MQCONN.

Pokud má ID uživatele adresního prostoru pouze přístup pro čtení, což je minimum, které vyžadujete k připojení ve všech, použije se konfigurace produktu **CHCKLOCL** jako zapsaná.

Pokud má ID uživatele adresního prostoru přístup UPDATE (nebo vyšší), pak konfigurace **CHCKLOCL** pracuje v *VOLITELNÝ* režimu. To znamená, že nemusíte zadávat ID uživatele a heslo, ale pokud ano, musí být ID uživatele a heslo platnou dvojicí.

### **Zabezpečení připojení je již konfigurováno pro správce front produktu z/OS**

Pokud je pro správce front produktu z/OS konfigurováno zabezpečení připojení a chcete, aby se produkt **CHCKLOCL** (*REQUIRED*) použil pro lokálně vázané aplikace WAS a žádné jiné, proveďte následující kroky:

1. Začni s **CHCKLOCL** (*VOLITELNÝ*) jako svou konfigurací. To znamená, že každé zadané ID uživatele a hesla se kontrolují na platnost, ale nejsou nařízeny.
2. Vypište všechny uživatele, kteří mají přístup k profilům zabezpečení připojení zadáním příkazu:

```
RLIST MQCONN MQ23.BATCH AUTHUSER
```

Tento příkaz se zobrazí například:

```
CLASS    NAME
-----  ----
MQCONN  MQ23.BATCH

USER     ACCESS  ACCESS COUNT
-----  -
JOHNDOE  READ     000009
JDOE1    READ     000003
WASUSER  READ     000000
```

3. Pro každé ID uživatele uvedené jako mající přístup pro čtení, změňte přístup na

```
UPDATE:- PERMIT MQ23.BATCH CLASS(MQCONN) ID(JOHNDOE) ACCESS(UPDATE)
```

4. Aktualizujte konfiguraci produktu IBM MQ na **CHCKLOCL** (*REQUIRED*).

Kombinace přístupu UPDATE k produktu MQ23.BATCH a aktuálního nastavení znamená, že používáte produkt **CHCKLOCL** (*VOLITELNÝ*).

5. Nyní použijte chování **CHCKLOCL** (*REQUIRED*) na jedno specifické ID uživatele, například WASUSER, takže všechna připojení přicházející z této oblasti musí poskytovat ID uživatele a heslo.
6. Proveďte to tím, že změníte dříve provedené změny zadáním následujícího příkazu:

```
PERMIT MQ23.BATCH CLASS(MQCONN) ID(WASUSER) ACCESS(READ)
```

## Zabezpečení připojení není konfigurováno pro správce front produktu z/OS

V této situaci musíte:

1. Vytvořte profily připojení pro produkt h1q.BATCH ve třídě MQCONN zadáním následujícího příkazu:

```
RDEFINE MQCONN MQ23.BATCH UACC(NONE)
```

2. Autorizujte všechna ID uživatelů, která vytvářejí dávková připojení ke správci front, aby měli k tomuto profilu přístup UPDATE. Tím dojde k vynechání požadavku **CHCKLOCL** (*REQUIRED*) pro ID uživatele a heslo v době připojení.
3. Proveďte to zadáním následujícího příkazu:

```
PERMIT MQ23.BATCH CLASS(MQCONN) ID(JOHNDOE) ACCESS(UPDATE)
```

Ty zahrnují ID uživatelů:

- a. Používá se pro panely CSQUTIL, ISPF a další lokálně vázané nástroje.
  - b. Přidruženo k dávkovému zpracování jako připojení ke správci front. Zvažte například příklad: IBM MQ Advanced Message Security, IBM Integration Bus, uložené procedury produktu Db2, uživatelé USS a TSO a aplikace Java.
4. Zadáním následujícího příkazu odstraňte profil přepínače pro správce front:

```
h1q.NO.CONNECT.CHECKS
```

- Nyní použijte chování **CHKLOCL** (*REQUIRED*) na jedno specifické ID uživatele, například WASUSER, takže všechna připojení přicházející z této oblasti musí poskytovat ID uživatele a heslo.
- Proveďte to tím, že změníte dříve provedené změny zadáním následujícího příkazu:

```
PERMIT MQ23.BATCH CLASS(MQCONN) ID(WASUSER) ACCESS(READ)
```

#### *Profily zabezpečení připojení pro připojení CICS*

Profily pro kontrolu připojení produktu CICS se skládají ze správce front nebo názvu skupiny sdílení front, za nímž následuje slovo *CICS* . Poskytněte ID uživatele přidružené k adresnímu prostoru CICS READ přístup k profilu připojení.

Profily pro kontrolu připojení z produktu CICS mají tento tvar:

```
hlq.CICS
```

kde hlq může být buď qmgr - name (název správce front), nebo qsg - name (název skupiny sdílení front). Používáte-li správce front i zabezpečení na úrovni skupiny sdílení front, produkt IBM MQ vyhledá profil s předponou názvu správce front. Pokud ji nenajde, hledá profil s předponou název skupiny sdílení front. Pokud se nepodaří najít žádný profil, požadavek na připojení selže.

Pro požadavky na připojení od CICS musíte povolit pouze přístup ID uživatele adresního prostoru CICS k profilu připojení.

Například následující příkazy RACF umožňují uživateli adresního prostoru CICS adresovat ID uživatele KCBCICS pro připojení ke správci front TQM1:

```
RDEFINE MQCONN TQM1.CICS UACC(NONE)  
PERMIT TQM1.CICS CLASS(MQCONN) ID(KCBCICS) ACCESS(READ)
```

#### *Profily zabezpečení připojení pro připojení IMS*

Profily pro kontrolu připojení produktu IMS se skládají ze správce front nebo názvu skupiny sdílení front, za nímž následuje slovo *IMS* . Zadejte ID uživatele pro řízení IMS a ID uživatelů závislých oblastí READ pro přístup k profilu připojení.

Profily pro kontrolu připojení z produktu IMS mají tento tvar:

```
hlq.IMS
```

kde hlq může být buď qmgr - name (název správce front), nebo qsg - name (název skupiny sdílení front). Používáte-li správce front i zabezpečení na úrovni skupiny sdílení front, produkt IBM MQ vyhledá profil s předponou názvu správce front. Pokud ji nenajde, hledá profil s předponou název skupiny sdílení front. Pokud se nepodaří najít žádný profil, požadavek na připojení selže.

Pro požadavky na připojení pomocí IMS povolte přístup k profilu připojení pro řídicí a uživatelská ID závislých oblastí produktu IMS .

Například následující příkazy RACF umožňují:

- ID uživatele oblasti IMS , IMSREG, pro připojení ke správci front TQM1.
- Uživatelé ve skupině BMPGRP k odeslání úloh BMP.

```
RDEFINE MQCONN TQM1.IMS UACC(NONE)
PERMIT TQM1.IMS CLASS(MQCONN) ID(IMSREG,BMPGRP) ACCESS(READ)
```

### *Profily zabezpečení připojení pro inicializátor kanálu*

Profily pro kontrolu připojení z inicializátoru kanálu se skládají ze správce front nebo názvu skupiny sdílení front následovaného slovem *CHIN*. Zadejte ID uživatele použité inicializátorem kanálu s přístupem k profilu připojení *READ* k profilu připojení.

Profily pro kontrolu připojení od inicializátoru kanálu mají následující tvar:

```
hlq.CHIN
```

kde *hlq* může být buď *qmgr*-name (název správce front), nebo *qsg*-name (název skupiny sdílení front). Používáte-li správce front i zabezpečení na úrovni skupiny sdílení front, produkt IBM MQ vyhledá profil s předponou názvu správce front. Pokud ji nenajde, hledá profil s předponou název skupiny sdílení front. Pokud se nepodaří najít žádný profil, požadavek na připojení selže.

Pro požadavky na připojení pomocí inicializátoru kanálu definujte přístup k profilu připojení pro ID uživatele použité adresním prostorem úlohy iniciátoru kanálu.

Například následující příkazy produktu RACF umožňují připojení adresního prostoru inicializátoru kanálu s ID uživatele *DQCTRL* k připojení ke správci front *TQM1*:

```
RDEFINE MQCONN TQM1.CHIN UACC(NONE)
PERMIT TQM1.CHIN CLASS(MQCONN) ID(DQCTRL) ACCESS(READ)
```

### **Profily pro zabezpečení fronty**

Je-li zabezpečení fronty aktivní, je třeba definovat profily v příslušných třídách a povolit k těmto profilům přístup nezbytné skupiny nebo ID uživatelů. Profily zabezpečení fronty jsou pojmenovány podle správce front nebo skupiny sdílení front a fronty, která má být otevřena.

Je-li zabezpečení fronty aktivní, musíte:

- Definujte profily ve třídách **MQQUEUE** nebo **GMQUEUE**, pokud používáte velké profily.
- Definujte profily ve třídách **MXQUEUE** nebo **GMXQUEUE** v případě použití smíšených profilů případu.
- Povolte nezbytné skupiny nebo ID uživatelů pro přístup k těmto profilům, aby mohli vydat požadavky rozhraní API produktu IBM MQ, které používají fronty.

Profily pro zabezpečení fronty mají formu:

```
hlq.queueaname
```


kde *hlq* může být buď *qmgr*-name (název správce front) nebo *qsg*-name (název skupiny sdílení front) a *queueaname* je název otevřené fronty, jak je uvedeno v deskriptoru objektu na volání *MQOPEN* nebo *MQPUT1*.

Profil s předponou v názvu správce front řídí přístup k jedné frontě v daném správci front. Profil s předponou názvu skupiny sdílení front řídí přístup k jedné nebo více frontám s daným názvem fronty ve všech správcích front v rámci skupiny sdílení front, nebo přístup ke sdílené frontě libovolného správce front v rámci skupiny. Tento přístup lze potlačit pro jednotlivé správce front definováním profilu úrovně správce front pro danou frontu v daném správci front.

Je-li váš správce front členem skupiny sdílení front a používáte-li správce front i zabezpečení na úrovni skupiny sdílení front, produkt IBM MQ nejprve zkontroluje profil s předponou názvu správce front. Pokud ji nenajde, hledá profil s předponou název skupiny sdílení front.

Používáte-li sdílené fronty, doporučuje se používat zabezpečení na úrovni skupiny sdílení front.

Podrobnosti o tom, jak zabezpečení fronty pracuje, je-li název fronty alias alias nebo fronty modelu

, viz [“Pokyny pro alias fronty”](#) na stránce 187 a [“Pokyny pro modelové fronty”](#) na stránce 188 .

Přístup RACF potřebný k otevření fronty závisí na zadaných volbách MQOPEN nebo MQPUT1 . Je-li více než jedna z voleb MQOO\_\* a MQPMO\_\* kódována, je kontrola zabezpečení fronty provedena pro nejvyšší požadované oprávnění RACF .

<i>Tabulka 31. Úrovně přístupu pro zabezpečení fronty pomocí volání MQOPEN nebo MQPUT1</i>	
<b>Volba MQOPEN nebo MQPUT1</b>	<b>RACF úroveň přístupu vyžadovaná pro přístup hlq.queueName</b>
MQOOK_BROWSE	READ (čtení)
MQO_DOTÁZAT SE	READ (čtení)
MQOO_BIND_*	AKTUALIZOVAT
MQO_INPUT_*	AKTUALIZOVAT
MQOO_OUTPUT nebo MQPUT1	AKTUALIZOVAT
MQOO_PASS_ALL_CONTEXT MQPMO_PASS_ALL_CONTEXT	AKTUALIZOVAT
MQOO_PASS_IDENTITY_CONTEXT MQPMO_PASS_IDENTITY_CONTEXT	AKTUALIZOVAT
ÁLNÍ_KONTEXT MQOO_SAVE_ALL_CONTEXT	AKTUALIZOVAT
MQOO_SET_IDENTITY_CONTEXT MQPMO_SET_IDENTITY_CONTEXT	AKTUALIZOVAT
MQO_SET_ALL_CONTEXT MQPMO_SET_ALL_CONTEXT	AKTUALIZOVAT
MQOOK_SADA	ALTER

Například u správce front IBM MQ QM77 mají být všechna ID uživatelů ve skupině RACF PAYGRP udělen přístup k získání zpráv z nebo vkládání zpráv do všech front s názvy začínajícími na 'PAY.'. To lze provést pomocí těchto příkazů obslužného programu RACF :

```
RDEFINE MQQUEUE QM77.PAY.** UACC(NONE)
PERMIT QM77.PAY.** CLASS(MQQUEUE) ID(PAYGRP) ACCESS(UPDATE)
```

Také všechna ID uživatelů ve skupině PAYGRP musí mít přístup k vkládání zpráv do front, které nepostupují podle konvence pojmenování PAY. Příklad:


```
REQUEST_QUEUE_FOR_PAYROLL
SALARY.INCREASE.SERVER
REPLIES.FROM.SALARY.MODEL
```

To lze provést definováním profilů pro tyto fronty ve třídě GMQQUEUE a zpřístupováním této třídy následujícím způsobem:

```
RDEFINE GMQQUEUE PAYROLL.EXTRAS UACC(NONE)
      ADDMEM(QM77.REQUEST_QUEUE_FOR_PAYROLL,
            QM77.SALARY_INCREASE.SERVER,
            QM77.REPLIES_FROM.SALARY.MODEL)
PERMIT PAYROLL.EXTRAS CLASS(GMQQUEUE) ID(PAYGRP) ACCESS(UPDATE)
```

**Poznámka:**

1. Pokud se změní úroveň přístupu produktu RACF , kterou má aplikace do profilu zabezpečení fronty, projeví se tyto změny pouze pro všechny nové získané popisovače objektů (tj. nové MQOPEN ) pro danou frontu. Tyto popisovače již existující v době změny si uchovají svůj stávající přístup do fronty. Je-li požadována aplikace pro použití změněné úrovně přístupu k frontě spíše než na existující úrovni přístupu, musí zavřít a znovu otevřít frontu pro každý popisovač objektu, který změnu vyžaduje.
2. V tomto příkladu může být název správce front QM77 také názvem skupiny sdílení front.

Další typy kontrol zabezpečení se mohou také vyskytnout v době otevření fronty v závislosti na zadaných volbách otevření a typech zabezpečení, které jsou aktivní.  Viz také “Profily pro zabezpečení kontextu” na stránce 202 a “Profily pro alternativní zabezpečení uživatelů” na stránce 201. U souhrnné tabulky zobrazující volby otevření a autorizace zabezpečení potřebné pro zařazení do fronty, kontext a alternativní zabezpečení uživatele jsou všechny aktivní, viz Tabulka 36 na stránce 193.

Pokud používáte publikování/odběr, je třeba vzít v úvahu následující informace: Při zpracování požadavku MQSUB je provedena kontrola zabezpečení, aby bylo zajištěno, že ID uživatele, který požadavek provádí, má požadovaný přístup k vkládání zpráv do cílové fronty IBM MQ a také požadovaný přístup k odběru tématu produktu IBM MQ .

<i>Tabulka 32. Úroveň přístupu pro zabezpečení fronty pomocí volání MQSUB</i>	
<b>Volba MQSUB</b>	<b>RACF úroveň přístupu vyžadovaná pro přístup hlq.queue name</b>
MQSO_ALTER, MQSO_CREATE, a MQSO_RESUME	AKTUALIZOVAT

**Poznámka:**

1. hlq . queue name je cílová fronta pro publikování. Pokud se jedná o spravovanou frontu, potřebujete přístup k příslušné modelové frontě, která má být použita pro spravovanou frontu a pro dynamickou frontu, která je vytvořena.
2. Tuto techniku můžete použít pro cílovou frontu, kterou jste zadali ve volání rozhraní MQSUB API, chcete-li rozlišovat mezi uživateli, kteří provádějí odběry, a uživateli, kteří načítají publikování z cílové fronty.

*Pokyny pro alias fronty*

Když vydáte volání MQOPEN nebo MQPUT1 pro frontu aliasů, provede produkt IBM MQ kontrolu prostředku proti názvu fronty uvedenému v deskriptoru objektu (MQOD) na volání. Nekontroluje, zda má uživatel povolen přístup k názvu cílové fronty.

Příklad: alias fronta s názvem PAYROLL.REQUEST se interpretuje jako cílová fronta PAY.REQUEST. Je-li zabezpečení fronty aktivní, musíte mít oprávnění pouze pro přístup ke frontě PAYROLL.REQUEST. Neprovede se žádná kontrola, abyste zjistili, zda máte oprávnění pro přístup do fronty PAY.REQUEST.

*Použití alias front k rozlišení mezi příkazy MQGET a MQPUT*

Rozsah volání MQI dostupných na jedné úrovni přístupu může způsobit problém, pokud chcete omezit přístup k frontě tak, aby povolovalo pouze volání **MQPUT** , nebo pouze volání **MQGET** . Fronta může



být chráněna definováním dvou aliasů, které se interpretují do fronty: jedna, která umožňuje aplikacím získávat zprávy z fronty, a to, které umožní aplikacím vkládat zprávy do fronty.

Následující text vám poskytuje příklad, jak můžete definovat fronty do produktu IBM MQ:

```
DEFINE QLOCAL(MUST_USE_ALIAS_TO_ACCESS) GET(ENABLED)
PUT(ENABLED)

DEFINE QALIAS(USE_THIS_ONE_FOR_GETS) GET(ENABLED)
PUT(DISABLED) TARGQ(MUST_USE_ALIAS_TO_ACCESS)

DEFINE QALIAS(USE_THIS_ONE_FOR_PUTS) GET(DISABLED)
PUT(ENABLED) TARGQ(MUST_USE_ALIAS_TO_ACCESS)
```

Musíte také provést následující definice RACF :

```
RDEFINE MQQUEUE hlq.MUST_USE_ALIAS_TO_ACCESS UACC(NONE)
RDEFINE MQQUEUE hlq.USE_THIS_ONE_FOR_GETS UACC(NONE)
RDEFINE MQQUEUE hlq.USE_THIS_ONE_FOR_PUTS UACC(NONE)
```

Poté zajistíte, aby žádný uživatel neměl přístup ke frontě hlq.MUST\_USE\_ALIAS\_TO\_ACCESS, a udělte příslušným uživatelům nebo skupinám přístup k aliasu. To lze provést pomocí následujících příkazů obslužného programu RACF :

```
PERMIT hlq.USE_THIS_ONE_FOR_GETS CLASS(MQQUEUE)
ID(GETUSER,GETGRP) ACCESS(UPDATE)
PERMIT hlq.USE_THIS_ONE_FOR_PUTS CLASS(MQQUEUE)
ID(PUTUSER,PUTGRP) ACCESS(UPDATE)
```

To znamená, že ID uživatele GETUSER a ID uživatelů ve skupině GETGRP je povoleno pouze pro získání zpráv o MUST\_USE\_ALIAS\_TO\_ACCESS prostřednictvím alias fronty USE\_THIS\_ONE\_FOR\_GETS; a ID uživatele PUTUSER a ID uživatele ve skupině PUTGRP jsou povoleny pouze pro vkládání zpráv prostřednictvím alias fronty USE\_THIS\_ONE\_FOR\_PUTS.

#### **Poznámka:**

1. Chcete-li použít techniku, jako je tato, musíte o tom informovat vývojáře aplikací, aby mohli vhodně navrhnout své programy.
2. Tuto techniku můžete použít pro frontu místa určení, kterou zadáte, a požadavek rozhraní API MQSUB, chcete-li rozlišovat mezi uživateli, kteří provádějí odběry, a tím, že uživatelé 'získali' publikování z cílové fronty.

#### *Pokyny pro modelové fronty*

Chcete-li otevřít modelovou frontu, musíte mít možnost otevřít jak samotnou modelovou frontu, tak i dynamickou frontu, na kterou se řeší. Definujte generické profily produktu RACF pro dynamické fronty, včetně dynamických front používaných obslužnými programy produktu IBM MQ .

Když otevřete modelovou frontu, zabezpečení produktu IBM MQ provede dvě kontroly zabezpečení fronty:

1. Jste autorizováni pro přístup k modelové frontě?
2. Jste autorizováni pro přístup k dynamické frontě, na kterou je modelová fronta vyřešena?

Pokud název dynamické fronty obsahuje koncový znak hvězdičky (\*), je tento znak \* nahrazen znakovým řetězcem generovaným produktem IBM MQ, aby se vytvořila dynamická fronta s jedinečným názvem. Protože se však pro kontrolu oprávnění používá celý název, včetně tohoto vygenerovaného řetězce, měli byste definovat generické profily pro tyto fronty.

Volání MQOPEN například používá název modelové fronty CREDIT.CHECK.REPLY.MODEL a název dynamické fronty CREDIT.REPLY.\* ve správci front (nebo ve skupině sdílení front) MQSP.

Chcete-li to provést, je třeba při definování nezbytných profilů fronty zadat následující příkazy produktu RACF :

```
RDEFINE MQQUEUE MQSP.CREDIT.CHECK.REPLY.MODEL
RDEFINE MQQUEUE MQSP.CREDIT.REPLY.**
```

Chcete-li umožnit uživateli přístup k těmto profilům, musíte také zadat odpovídající příkazy RACF PERMIT.

Typický název dynamické fronty vytvořený pomocí MQOPEN je něco jako CREDIT.REPLY.A346EF00367849A0. Přesná hodnota posledního kvalifikátoru je nepředvídatelná; proto byste měli používat generické profily pro tyto názvy front.

Počet zpráv obslužných programů produktu IBM MQ vkládaného do dynamických front. Profily byste měli definovat pro následující dynamické názvy front a poskytnout přístup pro příkaz RACF UPDATE k příslušným ID uživatelů (viz [“ID uživatele pro kontrolu zabezpečení”](#) na stránce 222 , kde jsou uvedena správná ID uživatelů):

```
SYSTEM.CSQUTIL.* (used by CSQUTIL)
SYSTEM.CSQOREXX.* (used by the operations and control panels)
SYSTEM.CSQXCMD.* (used by the channel initiator when processing CSQINPX)
CSQ4SAMP.* (used by the WebSphere MQ supplied samples)
```

Můžete také zvážit definování profilu pro řízení použití dynamického názvu fronty použitého při výchozím nastavení v členech programu pro kopírování aplikací. Kopírovací knihy dodané IBM MQ obsahují výchozí *DynamickáQName*, což je CSQ.\*. Tím je umožněno vytvoření odpovídajícího profilu RACF .

**Poznámka:** Nepovolujte programátorům aplikací zadat pro název dynamické fronty hodnotu jedinou \*. Pokud ano, musíte definovat hlq. \*\* profilu ve třídě MQQUEUE a vy jej budete muset poskytnout v rámci přístupu k přístupu. To znamená, že tento profil může být použit i pro jiné nedynamické fronty, které nemají specifitější profil RACF . Vaši uživatele tak mohou získat přístup k frontám, do kterých nechcete, aby měli přístup.

#### Volby zavření u trvalých dynamických front

Pokud aplikace otevře trvalou dynamickou frontu, která byla vytvořena jinou aplikací, a poté se pokusí tuto frontu odstranit s volbou MQCLOSE , uplatní se při pokusu o další kontroly zabezpečení.

Tabulka 33. Úroveň přístupu pro trvalé volby v trvalých dynamických frontách	
volba MQCLOSE	Úroveň přístupu produktu RACF je vyžadována pro hlq.queueName .
MQCO_DELETE	ALTER
MQCO_DELETE_PURGE	ALTER

#### Zabezpečení a vzdálené fronty

Když je zpráva vložena do vzdálené fronty, závisí zabezpečení fronty, které je implementováno lokálním správcem front, na tom, jak je vzdálená fronta zadána při jeho otevření.

Jsou použita následující pravidla:

1. Pokud byla vzdálená fronta definována v lokálním správci front prostřednictvím příkazu IBM MQ DEFINE QREMOTE, je zaškrtnutá fronta názvem vzdálené fronty. Je-li například ve správci front MQS1 definována vzdálená fronta, postupujte takto:

```
DEFINE QREMOTE (BANK7.CREDIT.REFERENCE)
RNAME (CREDIT.SCORING.REQUEST)
RQNAME (BNK7)
XMITQ (BANK1.TO.BANK7)
```

V tomto případě profil pro BANK7.CREDIT.REFERENCE musí být definován ve třídě MQQUEUE.

2. Pokud se položka *ObjectQMgr* pro daný požadavek neinterpretuje jako lokální správce front, provede se kontrola zabezpečení nad vyřešeným (vzdáleným) názvem správce front s výjimkou fronty klastru, v níž je provedena kontrola nad názvem fronty klastru.

Například přenosová fronta BANK1.TO.BANK7 je definován ve správci front MQS1. Požadavek MQPUT1 se pak vydá na MQS1 uvedením *ObjectName* jako BANK1.INTERBANK.TRANSFERS a *ObjectQMgrName* prvku BANK1.TO.BANK7. V takovém případě musí mít uživatel provádějící požadavek přístup k BANK1.TO.BANK7.

3. Provedete-li požadavek MQPUT na frontu a zadáte *ObjectQMgrName* jako název aliasu lokálního správce front, zkontroluje se zabezpečení pouze u názvu fronty, nikoli u správce front.

Když se zpráva dostane do vzdáleného správce front, může být předmětem dalšího zabezpečení zpracování. Další informace viz [“Zabezpečení pro vzdálený systém zpráv”](#) na stránce 82.

#### *Zabezpečení fronty nedoručených zpráv*

Speciální pokyny platí pro frontu nedoručených zpráv, protože mnoho uživatelů musí mít možnost vkládat zprávy do fronty, ale přístup k načítaným zprávám musí být přísně omezen. Toho lze dosáhnout použitím různých oprávnění správce RACF k frontě nedoručených zpráv a alias fronty.

Nedoručené zprávy lze vložit do speciální fronty s názvem fronty nedoručených zpráv. Pokud máte citlivá data, která by mohla skončit v této frontě, musíte vzít v úvahu její důsledky, protože nechcete, aby uživatelé tyto údaje načetli neautorizovaní uživatelé.

Každá z následujících položek musí mít povoleno vkládat zprávy do fronty nedoručených zpráv:

- Aplikační programy.
- Adresní prostor inicializátoru kanálu a všechna ID uživatele MCA. (Pokud profil RESLEVEL není přítomen nebo je definován tak, že ID uživatele kanálu jsou zaškrtnuty, ID uživatele kanálu také potřebuje oprávnění k umístění zpráv do fronty nedoručených zpráv.)
- CKTI, the CICS-supplied CICS task initiator.
- CSQQTRMN, the IBM MQ-supplied IMS trigger monitor.

Jediná aplikace, která může načítat zprávy z fronty nedoručených zpráv, by měla být 'speciální' aplikace, která zpracovává tyto zprávy. Problém však vzniká v případě, že poskytnete aplikacím RACF UPDATE oprávnění pro frontu nedoručených zpráv pro MQPUT , protože pak mohou automaticky načítat zprávy z fronty pomocí volání MQGET . Nemůžete zakázat frontu nedoručených zpráv pro operace get, protože pokud ano, ani ty 'speciální' aplikace nemohou načíst zprávy.

Jedním řešením tohoto problému je nastavit dvouúrovňový přístup k frontě zablokovaných dopisů. CKTI, transakce agenta kanálu zpráv nebo adresní prostor iniciátoru kanálu a 'speciální' aplikace mají přímý přístup; ostatní aplikace mohou přistupovat k frontě zablokovaných zpráv pouze prostřednictvím alias fronty. Tento alias je definován tak, aby povoloval aplikacím vkládat zprávy do fronty nedoručených zpráv, ale neodesílat zprávy z něj.

Takto by to mohlo fungovat:

1. Definujte skutečnou frontu nedoručených zpráv s atributy PUT (ENABLED) a GET (ENABLED), jak je zobrazeno v ukázce thlqual.SCSQPROC(CSQ4INYG).
2. Poskytněte oprávnění RACF UPDATE pro frontu nedoručených zpráv pro následující ID uživatelů:
  - ID uživatele, pod kterými běží CKTI a MCAs nebo adresní prostor iniciátoru kanálu.
  - ID uživatelů přidružená ke zpracování 'speciální' fronty zpracování nedoručených zpráv.
3. Definujte frontu aliasů, která bude převedena na skutečnou frontu nedoručených zpráv, ale dejte alias frontu těchto atributů: PUT (ENABLED) a GET (DISABLED). Zadejte alias fronty název se stejným kmenem jako název fronty nedoručených zpráv, ale připojte znaky ". PUT" k tomuto kmeni. Je-li například název fronty s dead-letter hlq.DEAD.QUEUE, alias fronty aliasů by byl hlq.DEAD.QUEUE.PUT.
4. Chcete-li vložit zprávu do fronty nedoručených zpráv, aplikace použije alias frontu. To musí vaše aplikace dělat:
  - Načtete název skutečné fronty nedoručených zpráv. Chcete-li tak učinit, otevře objekt správce front pomocí příkazu MQOPEN a poté vydá příkaz MQINQ , aby získal název fronty nedoručených zpráv.

- Sestavte název fronty aliasů přidáním znaků '.PUT' do tohoto názvu, v tomto případě, hlq.DEAD.QUEUE.PUT.
  - Otevřete alias frontu hlq.DEAD.QUEUE.PUT.
  - Vložte zprávu do fronty skutečných nedoručených zpráv tak, že zadáte příkaz MQPUT k alias fronty.
5. Poskytněte ID uživatele přidružené k aplikaci RACF UPDATE oprávnění k aliasu, ale nemá přístup (oprávnění NONE) k skutečné frontě nedoručených zpráv. To znamená, že:
- Aplikace může vkládat zprávy do fronty nedoručených zpráv pomocí fronty aliasů.
  - Aplikace nemůže načíst zprávy z fronty nedoručených zpráv s použitím fronty aliasů, protože fronta aliasů je zakázána pro operace get.

Aplikace nemůže získat žádné zprávy ze skutečné fronty nedoručených zpráv, protože má správné oprávnění RACF .

Tabulka 34 na stránce 191 shrnuje oprávnění RACF požadované pro různé účastníky tohoto řešení.

<i>Tabulka 34. Oprávnění správce RACF k frontě nedoručených zpráv a její alias</i>		
<b>ID přidružených uživatelů</b>	<b>Skutečná fronta nedoručených zpráv (hlq.DEAD.QUEUE)</b>	<b>Alias fronta nedoručených zpráv (hlq.DEAD.QUEUE.PUT)</b>
Název adresního prostoru MCA nebo inicializátor kanálu a CKTI	AKTUALIZOVAT	ŽÁDNÉ
'Speciální' aplikace (pro zpracování fronty nedoručených zpráv)	AKTUALIZOVAT	ŽÁDNÉ
ID uživatele aplikace zapsaná uživatelem	ŽÁDNÉ	AKTUALIZOVAT

Použijete-li tuto metodu, aplikace nemůže určit maximální délku zprávy (MAXMSGL) ve frontě nedoručených zpráv. Důvodem je skutečnost, že atribut MAXMSGL nelze načíst z alias fronty. Proto by vaše aplikace měla předpokládat, že maximální délka zprávy je 100 MB, maximální velikost IBM MQ for z/OS podporuje. Skutečná fronta nedoručených zpráv by měla být také definována s atributem MAXMSGL o velikosti 100 MB.

**Poznámka:** Uživatelem napsané aplikační programy obvykle nepoužívají alternativní oprávnění uživatele k umístění zpráv do fronty nedoručených zpráv. Tím se sníží počet ID uživatelů, kteří mají přístup k frontě nedoručených zpráv.

#### *Zabezpečení systémové fronty*

Chcete-li povolit určitým systémovým frontám přístup ke konkrétním systémovým frontám, je třeba nastavit přístup produktu RACF .

Pomocným částem IBM MQpřistupuje k mnoha frontám systému:

- Obslužný program CSQUTIL
- Ovládací panely a ovládací panely
- Adresní prostor inicializátoru kanálu (včetně démona publikování/odběru ve frontě)

ID uživatelů, pod kterým tyto spuštění musí být udělen RACF přístup k těmto frontám, jak je zobrazeno v [Tabulka 35 na stránce 192](#).

Tabulka 35. Přístup požadovaný pro fronty SYSTEM pomocí IBM MQ

Fronta SYSTEM	KALKUNIT	CSQUTIL	Ovládací panely a ovládací panely	Inicializátor kanálu pro distribuované fronty
SYSTEM.ADMIN.CHANNEL.EVENT	-	-	-	AKTUALIZOVAT
SYSTEM.BROKER.ADMIN.STREAM	-	-	-	ALTER
SYSTEM.BROKER.CONTROL.QUEUE	-	-	-	ALTER
SYSTEM.BROKER.DEFAULT.STREAM	-	-	-	ALTER
SYSTEM.BROKER.INTER.BROKER.COMMUNICATIONS	-	-	-	AKTUALIZOVAT
SYSTEM.CHANNEL.INITQ	-	-	-	AKTUALIZOVAT
SYSTEM.CHANNEL.SYNCQ	-	-	-	AKTUALIZOVAT
SYSTEM.CLUSTER.COMMAND.QUEUE	-	-	-	ALTER
SYSTEM.CLUSTER.REPOSITORY.QUEUE	-	-	-	AKTUALIZOVAT
SYSTEM.CLUSTER.TRANSMIT.QUEUE	-	-	-	ALTER
SYSTEM.COMMAND.INPUT	AKTUALIZOVAT	-	AKTUALIZOVAT	AKTUALIZOVAT
SYSTEM.COMMAND.REPLY.*	-	-	-	AKTUALIZOVAT
SYSTEM.COMMAND.REPLY.MODEL	AKTUALIZOVAT	-	AKTUALIZOVAT	AKTUALIZOVAT
SYSTEM.CSQOREXX.*	-	-	AKTUALIZOVAT	-
SYSTEM.CSQUTIL.*	AKTUALIZOVAT	-	-	-
SYSTEM.CSQXCMD.*	-	-	-	AKTUALIZOVAT
SYSTEM.HIERARCHY.STATE	-	-	-	AKTUALIZOVAT
SYSTEM.INTER.QMGR.CONTROL	-	-	-	AKTUALIZOVAT
SYSTEM.INTER.QMGR.PUBS	-	-	-	AKTUALIZOVAT
SYSTEM.INTER.QMGR.FANREQ	-	-	-	AKTUALIZOVAT
SYSTEM.PROTECTION.ERROR.QUEUE	-	-	-	AKTUALIZOVAT

Tabulka 35. Přístup požadovaný pro fronty SYSTEM pomocí IBM MQ (pokračování)

Fronta SYSTEM	KALKUNIT	C S Q U T I L	Ovládací panely a ovládací panely	Inicializátor kanálu pro distribuované fronty
SYSTEM.PROTECTION.POLICY.QUEUE	-	A K T U A L I Z O V A T ( <u>1</u> )	-	READ (čtení)
SYSTEM.QSG.CHANNEL.SYNCQ	-	-	-	AKTUALIZOVAT
SYSTEM.QSG.TRANSMIT.QUEUE	-	-	-	AKTUALIZOVAT

Rozhraní API-rychlý odkaz na zabezpečení přístupu k prostředkům

Souhrn voleb **MQOPEN**, **MQPUT1**, **MQSUB** a **MQCLOSE** a přístup požadovaný různými typy zabezpečení prostředků.

Tabulka 36. Volby MQOPEN, MQPUT1, MQSUB a MQCLOSE a požadovaná autorizace zabezpečení. Bublíny zobrazené jako tento **(1)** odkazují na poznámky následující za touto tabulkou.

Požadovaná minimální úroveň přístupu RACF				
RACF Třída:	MXTOPIC	MQQUEUE nebo MXQUEUE ( <u>1</u> )	MQADMIN nebo MXADMIN	MQADMIN nebo MXADMIN
RACF Profil:	( <u>15</u> nebo <u>16</u> )	( <u>2</u> )	( <u>3</u> )	( <u>4</u> )
Volba MQOPEN				
MQO_DOTÁZAT SE		READ ( <u>5</u> )	Žádná kontrola	Žádná kontrola
MQOOK_BROWSE		READ (čtení)	Žádná kontrola	Žádná kontrola
MQO_INPUT_*		AKTUALIZOVA T	Žádná kontrola	Žádná kontrola
MQOO_SAVE_ALL_CONTEXT ( <u>6</u> )		AKTUALIZOVA T	Žádná kontrola	Žádná kontrola
MQOO_OUTPUT (USAGE = NORMAL) ( <u>7</u> )		AKTUALIZOVA T	Žádná kontrola	Žádná kontrola

Tabulka 36. Volby MQOPEN, MQPUT1, MQSUB a MQCLOSE a požadovaná autorizace zabezpečení. Bubliny zobrazené jako tento (1) odkazují na poznámky následující za touto tabulkou. (pokračování)

Požadovaná minimální úroveň přístupu RACF				
RACF Třída:	MXTOPIC	MQQUEUE nebo MXQUEUE ( 1 )	MQADMIN nebo MXADMIN	MQADMIN nebo MXADMIN
RACF Profil:	( 15 nebo 16 )	( 2 )	( 3 )	( 4 )
MQOO_PASS_IDENTITY_CONTEXT ( 8 )		AKTUALIZOVAT	READ (čtení)	Žádná kontrola
MQOO_PASS_ALL_CONTEXT ( 8 ) ( 9 )		AKTUALIZOVAT	READ (čtení)	Žádná kontrola
MQOO_SET_IDENTITY_CONTEXT ( 8 ) ( 9 )		AKTUALIZOVAT	AKTUALIZOVAT	Žádná kontrola
MQOO_SET_ALL_CONTEXT ( 8 ) ( 10 )		AKTUALIZOVAT	CONTROL	Žádná kontrola
MQOO_OUTPUT (USAGE (XMITQ) ( 11 )		AKTUALIZOVAT	CONTROL	Žádná kontrola
MQOO_OUTPUT (objekt tématu)	UPDATE ( 16 )			
MQOO_OUTPUT (alias fronty k objektu tématu)	UPDATE ( 16 )	AKTUALIZOVAT		
MQOOK_SADA		ALTER	Žádná kontrola	Žádná kontrola
MQO_ALTERNATE_USER_AUTHORITY.		( 12 )	( 12 )	AKTUALIZOVAT
Volba MQPUT1				
Vložení do normální fronty ( 7 )		AKTUALIZOVAT	Žádná kontrola	Žádná kontrola
KONTEXT MQPMO_PASS_IDENTITY_CONTEXT		AKTUALIZOVAT	READ (čtení)	Žádná kontrola
MQPMO_PASS_ALL_CONTEXT		AKTUALIZOVAT	READ (čtení)	Žádná kontrola
KONTEXT MQPMO_SET_IDENTITY_CONTEXT		AKTUALIZOVAT	AKTUALIZOVAT	Žádná kontrola
MQPMO_SET_ALL_CONTEXT		AKTUALIZOVAT	CONTROL	Žádná kontrola
MQOOK_VÝSTUP		AKTUALIZOVAT	CONTROL	Žádná kontrola
Vložení do přenosové fronty ( 11 )				
MQOO_OUTPUT (objekt tématu)	UPDATE ( 16 )			
MQOO_OUTPUT (alias fronty k objektu tématu)	UPDATE ( 16 )	AKTUALIZOVAT		
MQPMO_ALTERNATE_USER_AUTHORITY		( 13 )	( 13 )	AKTUALIZOVAT

Tabulka 36. Volby MQOPEN, MQPUT1, MQSUB a MQCLOSE a požadovaná autorizace zabezpečení. Bubliny zobrazené jako tento (1) odkazují na poznámky následující za touto tabulkou. (pokračování)

Požadovaná minimální úroveň přístupu RACF				
RACF Třída:	MXTOPIC	MQQUEUE nebo MXQUEUE ( 1 )	MQADMIN nebo MXADMIN	MQADMIN nebo MXADMIN
RACF Profil:	( 15 nebo 16 )	( 2 )	( 3 )	( 4 )
Volba MQCLOSE				
MQCO_DELETE ( 14 )		ALTER	Žádná kontrola	Žádná kontrola
MQCO_DELETE_PURGE ( 14 )		ALTER	Žádná kontrola	Žádná kontrola
MQCO_REMOVE_SUB	ALTER ( 15 )			
Volba MQSUB				
VYTVOŘENÉ MQSO_CREATE	ALTER ( 15 )	( 17 )	( 18 )	
MQSO_ALTER	ALTER ( 15 )	( 17 )	( 18 )	
MQSO_RESUME	READ ( 15 )	( 17 )	Žádná kontrola	
OPRÁVNĚNÍ UŽIVATELE MQSO_ALTERNATE_USER_AUTHORITY				AKTUALIZOVAT
KONTEXT MQSO_SET_IDENTITY_CONTEXT			( 18 )	

**Poznámka:**

1. Tato volba není omezena na fronty. Použijte třídu MQNLIST nebo MXNLIST pro seznamy názvů a třídu MQPROC nebo MXPROC pro procesy.
2. Použít profil produktu RACF : hlq.resourcenam
3. Použijte profil produktu RACF : hlq.CONTEXT.queueam
4. Použijte profil produktu RACF : hlq.ALTERNATE.USER. alternateuserid  
alternateuserid je identifikátor uživatele, který je zadán v poli *AlternateUserId* v deskriptoru objektu. Všimněte si, že pro tuto kontrolu se použije až 12 znaků z pole *AlternateUserId*, na rozdíl od jiných kontrol, kde se používají pouze prvních 8 znaků identifikátoru uživatele.
5. Při otevírání správce front pro dotazy se nekontroluje žádná kontrola.
6. Musí být zadán také parametr MQOO\_INPUT\_\*. Toto je platné pro lokální, modelovou nebo alias frontu.
7. Tato kontrola se provádí pro lokální nebo modelovou frontu, která má atribut fronty *Usage* MQUS\_NORMAL, a také pro alias nebo vzdálenou frontu (která je definována pro připojeného správce front). Je-li fronta vzdálenou frontou, která je otevřena zadáním *ObjectQMGrName* (nikoli názvu připojeného správce front) explicitně, provede se kontrola ve frontě se stejným názvem jako *ObjectQMGrName* (což musí být lokální fronta s atributem fronty *Usage* MQUS\_TRANSMISION).
8. Musí být zadán také MQOO\_OUTPUT.
9. Tuto volbu má také implikovaná hodnota MQO\_P\_PASS\_IDENTITY\_CONTEXT.
10. Tato volba zahrnuje i MQOO\_PASS\_IDENTITY\_CONTEXT, MQOO\_PASS\_ALL\_CONTEXT a MQOO\_SET\_IDENTITY\_CONTEXT.



11. Tato kontrola se provádí pro lokální nebo modelovou frontu, která má atribut fronty *Usage* MQUS\_TRANSMISSION, a je otevírány přímo pro výstup. Nepoužije se, je-li otevřena vzdálená fronta.
12. Musí být zadán alespoň jeden z příkazů MQOO\_INQUIRE, MQOO\_BROWSE, MQOO\_INPUT\_\*, MQOO\_OUTPUT nebo MQOO\_SET. Kontrola prováděná je stejná jako u ostatních zadaných voleb.
13. Kontrola prováděná je stejná jako u ostatních zadaných voleb.
14. Toto platí pouze pro trvalé dynamické fronty, které byly otevřeny přímo, tj. neotevřené přes modelovou frontu. K odstranění dočasné dynamické fronty není vyžadováno žádné zabezpečení.
15. Použijte profil produktu RACF hlq.SUBSCRIBE.topicname.
16. Použijte profil produktu RACF hlq.PUBLISH.topicname.
17. Pokud jste v požadavku MQSUB zadali cílovou frontu pro publikování, která má být odeslána, provede se kontrola zabezpečení proti této frontě, abyste se ujistili, že jste do této fronty zadali oprávnění.
18. Pokud v požadavku MQSUB s uvedenými volbami MQSO\_CREATE nebo MQSO\_ALTER chcete nastavit libovolné pole kontextu identity ve struktuře MQSD, je nutné zadat také volbu MQSO\_SET\_IDENTITY\_CONTEXT a také pro cílovou frontu potřebujete příslušné oprávnění k profilu kontextu.

### Profily pro zabezpečení témat

Je-li zabezpečení tématu aktivní, je třeba definovat profily v příslušných třídách a povolit k těmto profilům přístup nezbytné skupiny nebo uživatelská jména.

Koncepce zabezpečení tématu v rámci stromu témat je popsána v tématu [Zabezpečení publikování/ odběru](#).

Je-li zabezpečení tématu aktivní, je třeba provést následující akce:

- Definujte profily ve třídách **MXTOPIC** nebo **GMXTOPIC**.
- Povolte k těmto profilům přístup nezbytné skupiny nebo ID uživatelů, aby mohli vydat požadavky rozhraní API produktu IBM MQ, které používají témata.

Profily pro zabezpečení témat mají tento tvar:

```
hlq.SUBSCRIBE.topicname
hlq.PUBLISH.topicname
```

kde:

- *hlq* je buď *qmgr-name* (název správce front), nebo *qsg-name* (název skupiny sdílení front).
- *topicname* je název uzlu administrace témat ve stromu témat přidružený buď k odběru tématu prostřednictvím volání MQSUB nebo je publikován prostřednictvím volání MQOPEN.

Profil s předponou v názvu správce front řídí přístup k jedinému tématu v daném správci front. Profil s předponou názvu skupiny sdílení front řídí přístup k jednomu nebo více tématům s daným názvem tématu ve všech správcích front v rámci skupiny sdílení front. Tento přístup lze potlačit pro jednotlivé správce front definováním profilu úrovně správce front pro dané téma v daném správci front.

Je-li váš správce front členem skupiny sdílení front a používáte-li správce front i zabezpečení na úrovni skupiny sdílení front, produkt IBM MQ nejprve zkontroluje profil s předponou názvu správce front. Pokud ji nenajde, hledá profil s předponou název skupiny sdílení front.

### Odebírat

Chcete-li se přihlásit k odběru tématu, musíte mít přístup k tématu, k jehož odběru se chcete přihlásit, a cílové fronty pro publikování.

Když zadáte požadavek MQSUB, dojde k následujícím kontrolám zabezpečení:

- Zda máte k dispozici příslušnou úroveň přístupu k odběru daného tématu a také že cílová fronta (je-li zadána) je otevřena pro výstup
- Zda máte odpovídající úroveň přístupu k této cílové frontě.

Tabulka 37. Úroveň přístupu vyžadovaná pro zabezpečení tématu k odběru

Akce	Požadovaná úroveň přístupu
MQSUB na téma	RACF access required to <i>hlq.SUBSCRIBE.topicname</i> profile in MXTOPIC class
MQSO_CREATE a MQSO_ALTER	ALTER
MQSO_RESUME	READ (čtení)
MQSUB-další oprávnění k nespravovaným cílovým frontám.	V třídě MQADMIN nebo MXADMIN je požadován přístup produktu RACF k profilu produktu <i>hlq.CONTEXT.queueName</i>
MQSO_CREATE, MQSO_ALTER, a MQSO_RESUME	AKTUALIZOVAT
	RACF přístup požadován k profilu produktu <i>hlq.queueName</i> ve třídě MQQUEUE nebo MXQUEUE
MQSO_CREATE a MQSO_ALTER	AKTUALIZOVAT
	V třídě MQADMIN nebo MXADMIN je požadován přístup produktu RACF k profilu produktu <i>hlq.ALTERNATE.USER.alternateuserid</i>
OPRÁVNĚNÍ UŽIVATELE MQSO_ALTERNATE_USER_AUTHORITY	AKTUALIZOVAT

## Pokyny pro spravované fronty pro odběry

Je provedena kontrola zabezpečení, abyste zjistili, zda máte oprávnění přihlásit se k odběru tématu. Při vytvoření spravované fronty se však neprovádějí žádné kontroly zabezpečení nebo pokud chcete určit, zda máte přístup k vkládání zpráv do této cílové fronty.

Nelze zavřít odstranění spravované fronty.

Použité modelové fronty jsou: SYSTEM.DURABLE.MODEL.QUEUE a SYSTEM.NDURABLE.MODEL.QUEUE.

Spravované fronty vytvořené z těchto modelových front jsou ve tvaru SYSTEM.MANAGED.DURABLE.A346EF00367849A0 a SYSTEM.MANAGED.NDURABLE.A346EF0036785EA0, kde je poslední kvalifikátor nepředvídatelný.

Neposkytujte žádné uživateli přístup k těmto frontám. Fronty mohou být chráněny pomocí generických profilů ve tvaru SYSTEM.MANAGED.DURABLE.\* a SYSTEM.MANAGED.NDURABLE.\* bez udělených oprávnění.

Zprávy lze z těchto front načíst pomocí manipulátoru vráceného v požadavku MQSUB.

Pokud jste explicitně zadali volání MQCLOSE pro odběr s určenou volbou MQCO\_REMOVE\_SUB a nevytvořili jste odběr, který jste uzavřeli pod tímto popisovačem, provede se kontrola zabezpečení v době uzavření, abyste se ujistili, že máte správné oprávnění k provedení této operace.

Tabulka 38. Úroveň přístupu vyžadovaná pro profily zabezpečení tématu pro uzavření operace odběru

Akce	Požadovaná úroveň přístupu
MQCLOSE (odběru)	RACF access required to <i>hlq.SUBSCRIBE.topicname</i> profile in MXTOPIC class
MQCO_REMOVE_SUB	ALTER

## Publikovat

Chcete-li publikovat na téma, které potřebujete k tématu, a pokud používáte alias fronty, také do fronty alias.

Akce	Požadovaná úroveň přístupu
MQOPEN (z tématu)	RACF access required to <i>hlq.PUBLISH.topicname</i> profile in MXTOPIC class
MQOO_OUTPUT nebo MQPUT1	AKTUALIZOVAT
MQOPEN (Fronta aliasů k tématu)	RACF přístup k profilu produktu <i>hlq.queueName</i> ve třídě MQQUEUE nebo MXQUEUE pro frontu aliasů
MQOO_OUTPUT nebo MQPUT1	AKTUALIZOVAT

Podrobnosti o tom, jak zabezpečení tématu funguje, když je otevřena fronta aliasů, která se řeší jako název tématu, je otevřena pro publikování, viz [“Aspekty pro fronty aliasů, které se interpretují na témata pro operaci publikování”](#) na stránce 198.

Při použití alias front aliasů použitých pro cílové fronty pro omezení PUT nebo GET viz [“Pokyny pro alias fronty”](#) na stránce 187.

Změní-li se úroveň přístupu produktu RACF na profil zabezpečení tématu, projeví se změny pouze u všech získaných nových manipulátorů objektů (tj. pro nové MQSUB nebo MQOPEN) daného tématu. Tyto popisovače již existující v době změny si uchovávají svůj stávající přístup k tématu. Také stávající odběratelé si uchovávají svůj přístup k veškerým odběrům, které již provedli.

## Aspekty pro fronty aliasů, které se interpretují na témata pro operaci publikování

Při zadání volání MQOPEN nebo MQPUT1 pro frontu aliasů, která je interpretována jako téma, produkt IBM MQ provede dvě kontroly prostředků:

- První z názvů alias fronty určených v deskriptoru objektu (MQOD) v rámci volání MQOPEN nebo MQPUT1 .
- Druhý proti tématu, na které se rozlišuje fronta aliasů

Musíte si být vědomi toho, že toto chování se liší od chování, které dostanete, když se alias fronty vyřeší do jiných front. Potřebujete správný přístup k oběma profilům, abyste mohli pokračovat v akci publikování.

## Zabezpečení tématu systému

K následujícím tématům systému je přístupován adresním prostorem inicializátoru kanálu.

ID uživatelů, pod kterými je toto spuštění spuštěno, musí mít přístup k těmto frontám RACF , jak je zobrazeno v [Tabulka 40](#) na stránce 198.

Téma SYSTEM	Profil	Inicializátor kanálu pro distribuované fronty
SYSTEM.BROKER.ADMIN.STREAM	PUBLISH.topicname	AKTUALIZOVAT
SYSTEM.BROKER.ADMIN.STREAM	SUBSCRIBE.topicname	ALTER

## Profily pro procesy

Je-li zabezpečení procesu aktivní, musíte definovat profily v odpovídajících třídách a povolit k těmto profilům přístup nezbytné skupiny nebo ID uživatelů.

Je-li zabezpečení procesu aktivní, musíte:

- Definujte profily ve třídách **MQPROC** nebo **GMQPROC** , pokud používáte velké profily.
- Definujte profily ve třídách **MXPROC** nebo **GMXPROC** v případě použití smíšených profilů případu.
- Povolte nezbytné skupiny nebo ID uživatelů pro přístup k těmto profilům, aby mohli vydávat požadavky rozhraní API produktu IBM MQ , které používají procesy.

Profily pro procesy mají tvar:

```
hlq.processname
```

kde hlq může být buď qmgr - name (název správce front), nebo qsg - name (název skupiny sdílení front) a processname je název otevíraný procesu.

Profil s předponou názvu správce front řídí přístup k jedné definici procesu v daném správci front. Profil s předponou názvu skupiny sdílení front řídí přístup k jedné nebo více definicím procesu s tímto názvem ve všech správcích front v rámci skupiny sdílení front. Tento přístup lze potlačit pro jednotlivé správce front definováním profilu úrovně správce front pro danou definici procesu v daném správci front.

Je-li váš správce front členem skupiny sdílení front a používáte-li správce front i zabezpečení na úrovni skupiny sdílení front, produkt IBM MQ nejprve zkontroluje profil s předponou názvu správce front. Pokud ji nenajde, hledá profil s předponou název skupiny sdílení front.

Následující tabulka zobrazuje přístup požadovaný pro otevření procesu.

Tabulka 41. Úroveň přístupu pro zabezpečení procesu	
Volba MQOPEN	Úroveň přístupu produktu RACF je vyžadována pro hlq.processname .
MQO_DOTAZAT SE	READ (čtení)

Například ve správci front MQS9 musí být skupina RACF INQVPRC schopna se dotázat (MQINQ) ve všech procesech začínajících písmenem V. Definice RACF by byly následující:

```
RDEFINE MQPROC MQS9.V* UACC(NONE)  
PERMIT MQS9.V* CLASS(MQPROC) ID(INQVPRC) ACCESS(READ)
```

Zabezpečení alternativního uživatele může být také aktivní v závislosti na otevřených volbách, které jsou zadány při otevření objektu definice procesu.

## Profily pro seznamy názvů

Je-li zabezpečení seznamu názvů aktivní, definujte profily v příslušných třídách a udělte těmto profilům přístup skupin nebo ID uživatelů.

Je-li zabezpečení seznamu názvů aktivní, musíte:

- Definujte profily ve třídách **MQNLIST** nebo **GMQNLIST** , pokud používáte velké profily.
- Definujte profily ve třídách **MXNLIST** nebo **GMXNLIST** v případě použití smíšených profilů případu.
- Povolte nezbytné skupiny nebo ID uživatelů pro přístup k těmto profilům.

Profily pro seznamy jmen mají tento tvar:

```
hlq.name-listname
```

kde hlq může být buď qmgr-name (název správce front), nebo qsg-name (název skupiny sdílení front) a namelistname je název seznamu názvů, který se má otevřít.

Profil s předponou názvu správce front řídí přístup k jednomu seznamu názvů v daném správci front. Profil začínající názvem skupiny sdílení front řídí přístup k jednomu nebo více seznamům názvů s tímto názvem ve všech správcích front v rámci skupiny sdílení front. Tento přístup lze potlačit pro jednotlivé správce front definováním profilu úrovně správce front pro daný seznam názvů v daném správci front.

Je-li váš správce front členem skupiny sdílení front a používáte-li správce front i zabezpečení na úrovni skupiny sdílení front, produkt IBM MQ nejprve zkontroluje profil s předponou názvu správce front. Pokud ji nenajde, hledá profil s předponou název skupiny sdílení front.

Následující tabulka zobrazuje přístup požadovaný pro otevření seznamu názvů.

<i>Tabulka 42. Úroveň přístupu pro zabezpečení seznamu názvů</i>	
<b>Volba MQOPEN</b>	<b>Úroveň přístupu RACF je vyžadována pro hlq.namelistname .</b>
MQO_DOTÁZAT SE	READ (čtení)

Například ve správci front (nebo ve skupině sdílení front) PQM3 musí být skupina RACF DEPT571 schopna zjišťovat (MQINQ) u těchto seznamů názvů:

- Všechny seznamy názvů začínající na "DEPT571".
- PRINTER/DESTINATIONS/DEPT571
- AGENTURA/ŽÁDOSTI/FRONTY
- WAREHOUSE.BROADCAST

Definice RACF k provedení této akce jsou:

```
RDEFINE MQNLIST PQM3.DEPT571.** UACC(NONE)
PERMIT PQM3.DEPT571.** CLASS(MQNLIST) ID(DEPT571) ACCESS(READ)

RDEFINE GMQNLIST NLISTS.FOR.DEPT571 UACC(NONE)
  ADDMEM(PQM3.PRINTER/DESTINATIONS/DEPT571,
        PQM3.AGENCY/REQUEST/QUEUES,
        PQM3.WAREHOUSE.BROADCAST)
PERMIT NLISTS.FOR.DEPT571 CLASS(GMQNLIST) ID(DEPT571) ACCESS(READ)
```

Alternativní zabezpečení uživatele může být aktivní v závislosti na volbách, které jsou určeny při otevření objektu seznamu názvů.

## Zabezpečení seznamu názvů systému

Mnoho systémů jmenovek systému je zpřístupněno pomocnými částmi produktu IBM MQ:

- Obslužný program CSQUTIL
- Ovládací panely a ovládací panely
- Adresní prostor inicializátoru kanálu (včetně démona publikování/odběru zařazeného ve frontě)

ID uživatelů, pod kterými jsou tyto spuštění spuštěny, musí mít RACF přístup k těmto seznamům názvů, jak je zobrazeno v části [Tabulka 43 na stránce 201](#).

Tabulka 43. Přístup k seznamům názvů SYSTEM vyžaduje produkt IBM MQ .

Seznam názvů SYSTEM	KALKUNIT	Ovládací panely a ovládací panely	Inicializátor kanálu pro distribuované fronty
SYSTEM.QPUBSUB.QUEUE.NAMELIST	-	-	READ (čtení)
SYSTEM.QPUBSUB.SUBPOINT.NAMELIST	-	-	READ (čtení)

### Profily pro alternativní zabezpečení uživatelů

Je-li zabezpečení alternativního uživatele aktivní, musíte definovat profily v odpovídajících třídách a povolit k těmto profilům přístup nezbytné skupiny nebo ID uživatelů.

Další informace o produktu *AlternateUserId* naleznete v části [AlternateUserID \(MQCHAR12\)](#).

Je-li zabezpečení alternativního uživatele aktivní, musíte:

- Definujte profily ve třídách MQADMIN nebo GMQADMIN, používáte-li velké profily.
- Definujte profily ve třídách MXADMIN nebo GMXADMIN, používáte-li smíšené profily případu.

Povolte potřebné skupiny nebo ID uživatelů pro přístup k těmto profilům, aby mohli při otevření objektu používat volby ALTERNATE\_USER\_AUTHORITY.

Profily pro alternativní zabezpečení uživatele lze zadat na úrovni subsystému nebo na úrovni skupiny sdílení front a mít následující formát:

```
hlq.ALTERNATE.USER.alternateuserid
```

Kde hlq může být buď qmgr-name (název správce front), nebo qsg-name (název skupiny sdílení front) a alternateuserid je hodnota pole *AlternateUserId* v deskriptoru objektu.

Profil s předponou názvu správce front řídí použití alternativního ID uživatele v daném správci front. Profil s předponou názvu skupiny sdílení front řídí použití alternativního jména uživatele ve všech správcích front v rámci skupiny sdílení front. Toto alternativní ID uživatele může být použito ve všech správcích front v rámci skupiny sdílení front uživatelem, který má správný přístup. Tento přístup lze u jednotlivých správců front potlačit definováním profilu úrovně správce front pro toto alternativní ID uživatele v daném správci front.

Je-li váš správce front členem skupiny sdílení front a používáte-li správce front i zabezpečení na úrovni skupiny sdílení front, produkt IBM MQ nejprve zkontroluje profil s předponou názvu správce front. Pokud ji nenajde, hledá profil s předponou název skupiny sdílení front.

Následující tabulka zobrazuje přístup při zadávání alternativní volby uživatele.

Tabulka 44. Úroveň přístupu pro zabezpečení alternativního uživatele	
Volby MQOPEN, MQSUB nebo MQPUT1	Je vyžadována úroveň přístupu RACF
MQO_ALTERNATE_USER_AUTHORITY MQSO_ALTERNATE_USER_AUTHORITY MQPMO_ALTERNATE_USER_AUTHORITY	AKTUALIZOVAT

Kromě alternativních kontrol zabezpečení uživatele lze také provést další kontroly zabezpečení pro frontu, proces, seznam názvů a kontext zabezpečení. Alternativní ID uživatele, je-li poskytnuto, se používá pouze pro kontroly zabezpečení ve frontě, definice procesu nebo prostředky seznamu názvů. Pro alternativní kontroly uživatele a zabezpečení kontextu se použije ID uživatele požadující, aby byla kontrola použita. Podrobnosti o tom, jak se zachází s ID uživatele, viz "ID uživatele pro kontrolu zabezpečení" na stránce 222. Pro souhrnnou tabulku zobrazující otevřené volby a bezpečnostní kontroly požadované, když jsou všechny aktivní fronty, kontext a alternativní zabezpečení uživatelů, viz [Tabulka 36 na stránce 193](#).

Alternativní uživatelský profil dává požadujícímu ID uživatele přístup k prostředkům přidruženým k ID uživatele uvedenému v alternativním ID uživatele. Například mzdový server spuštěný pod ID uživatele PAYSERV na správci front QMPY zpracovává požadavky od personálních ID uživatelů, přičemž všechny začínají na PS. Chcete-li zajistit, aby práce prováděná serverem mezd byla provedena pod ID uživatele požadujícího uživatele, použije se alternativní oprávnění uživatele. Výplatní server ví, které ID uživatele má být zadáno jako alternativní ID uživatele, protože požadující programy generují zprávy pomocí volby zprávy příkazu MQPMO\_DEFAULT\_CONTEXT. Další podrobnosti o tom, odkud získáte alternativní ID uživatelů, najdete v tématu [“ID uživatele pro kontrolu zabezpečení”](#) na stránce 222 .

Následující příklad definice RACF umožňuje programu serveru zadat alternativní ID uživatele začínající znaky PS:

```
RDEFINE MQADMIN QMPY.ALTERNATE.USER.PS* UACC(NONE)
PERMIT QMPY.ALTERNATE.USER.PS* CLASS(MQADMIN) ID(PAYSERV) ACCESS(UPDATE)
```

#### Poznámka:

1. Pole *AlternateUserId* v deskriptoru objektu a deskriptoru odběru jsou dlouhá 12 bajtů. Všech 12 bajtů se použije při kontrolách profilu, ale pouze prvních 8 bajtů se použije jako ID uživatele pro IBM MQ. Není-li toto oseknutí ID uživatele žádoucí, aplikační programy, které vyžadují požadavek, musí přeložit jakékoli alternativní ID uživatele o více než 8 bajtů do něčeho vhodnějšího.
2. Uvedete-li MQO\_ALTERNATE\_USER\_AUTHORITY, MQSO\_ALTERNATE\_USER\_AUTHORITY nebo MQPMO\_ALTERNATE\_USER\_AUTHORITY a nezádáte do deskriptoru objektu pole *AlternateUserId*, použije se ID uživatele mezery. Pro účely alternativního zabezpečení uživatele zkontrolujte, zda ID uživatele použité pro kvalifikátor *AlternateUserId* je -BLANK-. Například RDEF MQADMIN hlq.ALTERNATE.USER.-BLANK-.

Pokud má uživatel povolen přístup k tomuto profilu, všechny další kontroly se provedou s ID uživatele, které je prázdné. Podrobnosti o prázdných ID uživatelů najdete v tématu [“Prázdné ID uživatele a úrovně UACC”](#) na stránce 230.

Správa alternativních ID uživatelů je snazší, máte-li konvence pojmenování pro ID uživatelů, která vám umožní používat generické alternativní uživatelské profily. Pokud tomu tak není, můžete použít funkci RACVARS produktu RACF . Podrobnosti o používání RACVARS najdete v příručce *z/OS SecureWay Security Server RACF Security Administrator's Guide*.

Je-li zpráva vložena do fronty, která byla otevřena s alternativním oprávněním uživatele a kontext zprávy byl vygenerován správcem front, je pole MQMD\_USER\_IDENTIFIER nastaveno na alternativní ID uživatele.

### **Profily pro zabezpečení kontextu**

Produkt IBM MQ používá profily pro řízení přístupu k kontextovým informacím specifickým pro konkrétní zprávu. Kontext je obsažen v deskriptoru zpráv (MQMD).

### **Použití profilů pro zabezpečení kontextu**

Je-li zabezpečení kontextu aktivní, musíte:

- Definujte profil ve třídě **MQADMIN**, pokud používáte velké profily.
- Definujte profil ve třídě **MXADMIN**, používáte-li smíšené profily případu.

Profil se nazývá hlq.CONTEXT.queueName, kde:

#### **hlq**

Může být buď qmgr-name (název správce front), nebo qsg-name (název skupiny sdílení front).

#### **QueueName**

Může se jednat buď o úplný název fronty, pro kterou chcete definovat profil kontextu, nebo generický profil.

Profil s předponou názvu správce front a s hodnotou \*\* zadaným jako název fronty umožňuje řízení kontextu zabezpečení kontextu ve všech frontách náležejících k tomuto správci front. Tento parametr lze u jednotlivých front přepsat definováním profilu na úrovni fronty pro kontext v dané frontě.

Profil s předponou názvu skupiny sdílení front a s názvem \*\* určeným jako název fronty umožňuje řízení pro kontext ve všech frontách náležejících ke správcům front v rámci skupiny sdílení front. Tento parametr lze u jednotlivých správců front přepsat definováním profilu úrovně správce front pro kontext v daném správci front zadáním profilu s předponou názvu správce front. Může být také potlačen na jednotlivé frontě uvedením profilu s příponou s názvem fronty.

Je-li váš správce front členem skupiny sdílení front a používáte-li správce front i zabezpečení na úrovni skupiny sdílení front, produkt IBM MQ nejprve zkontroluje profil s předponou názvu správce front. Pokud ji nenajde, hledá profil s předponou název skupiny sdílení front.

Musíte dát nezbytné skupiny nebo ID uživatele přístup k tomuto profilu. Následující tabulka zobrazuje požadovanou úroveň přístupu v závislosti na specifikaci kontextových voleb při otevření fronty.

<i>Tabulka 45. Úrovně přístupu pro zabezpečení kontextu</i>	
<b>Volba MQOPEN nebo MQPUT1</b>	<b>Úroveň přístupu produktu RACF vyžadovaná pro hlq.CONTEXT.queueName</b>
MQPMOTO_NE_KONTEXT	Žádná kontrola zabezpečení kontextu
MQPMO_VÝCHOZÍ_KONTEXT	Žádná kontrola zabezpečení kontextu
ÁLNÍ_KONTEXT MQOO_SAVE_ALL_CONTEXT	Žádná kontrola zabezpečení kontextu
MQOO_PASS_IDENTITY_CONTEXT MQPMO_PASS_IDENTITY_CONTEXT	READ (čtení)
MQOO_PASS_ALL_CONTEXT MQPMO_PASS_ALL_CONTEXT	READ (čtení)
MQOO_SET_IDENTITY_CONTEXT MQPMO_SET_IDENTITY_CONTEXT	AKTUALIZOVAT
MQO_SET_ALL_CONTEXT MQPMO_SET_ALL_CONTEXT	CONTROL
MQOO_OUTPUT nebo MQPUT1(POUŽITÍ (XMITQ))	CONTROL
<b>Volba MQSUB</b>	
MQSO_SET_IDENTITY_CONTEXT ( <b>Poznámka 2</b> )	AKTUALIZOVAT

**Poznámka:**

1. ID uživatelů použitá pro distribuované ukládání do fronty vyžadují k umístění zpráv do cílové fronty přístup CONTROL ke správci hlq.CONTEXT.queueName. Chcete-li získat informace o použitých ID uživatelů, prohlédněte si příručku "ID uživatele použitá iniciátořem kanálu" na stránce 225.
2. Pokud v požadavku MQSUB s uvedenými volbami MQSO\_CREATE nebo MQSO\_ALTER chcete nastavit kterékoli z polí kontextu identity ve struktuře MQSD, je třeba určit volbu MQSO\_SET\_IDENTITY\_CONTEXT. Požadujete také odpovídající oprávnění ke kontextovému profilu pro cílovou frontu.

Pokud příkazy vložíte do vstupní fronty příkazů systému, použijte k přidružení správného ID uživatele k příkazu výchozí kontextovou volbu pro zprávu.

Například obslužný program dodaný IBM MQCSQUTIL může být použit k odlehčování a opětovnému načtení zpráv ve frontách. Jsou-li odložené zprávy obnoveny do fronty, obslužný program CSQUTIL použije volbu MQOO\_SET\_ALL\_CONTEXT k vrácení zpráv do původního stavu. Kromě zabezpečení fronty, které je vyžadováno touto volbou otevření, je také vyžadováno oprávnění ke kontextu. Je-li například toto oprávnění vyžadováno skupinou BACKGRP ve správci front MQS1, bude to definováno následujícím způsobem:



```
RDEFINE MQADMIN MQS1.CONTEXT.** UACC(NONE)
PERMIT MQS1.CONTEXT.** CLASS(MQADMIN) ID(BACKGRP) ACCESS(CONTROL)
```

V závislosti na uvedených volbách a typech provedených zabezpečení se při otevření fronty mohou vyskytnout i jiné typy kontrol zabezpečení. Patří k nim zabezpečení fronty (viz “Profily pro zabezpečení fronty” na stránce 185) a alternativní zabezpečení uživatelů (viz “Profily pro alternativní zabezpečení uživatelů” na stránce 201). Pro souhrnnou tabulku zobrazující otevřené volby a bezpečnostní kontroly požadované, když jsou všechny aktivní fronty, kontext a alternativní zabezpečení uživatelů, viz [Tabulka 36](#) na stránce 193.

## Zabezpečení kontextu systémové fronty

Většina systémových front je přístupováno pomocnými částmi IBM MQ, například adresním prostorem inicializátoru kanálu.

ID uživatelů, pod kterými je toto spuštění spuštěno, musí mít přístup k těmto frontám RACF, jak je zobrazeno v [Tabulka 46](#) na stránce 204.

<i>Tabulka 46. Přístup požadovaný k frontám SYSTEM pro operace kontextu</i>	
<b>Fronta SYSTEM</b>	<b>Inicializátor kanálu pro distribuované fronty</b>
SYSTEM.BROKER.CONTROL.QUEUE	CONTROL
SYSTEM.BROKER.INTER.BROKER.COMMUNICATIONS	CONTROL
SYSTEM.CHANNEL.SYNCQ	CONTROL
SYSTEM.CLUSTER.TRANSMIT.QUEUE	CONTROL

### **Profily pro zabezpečení příkazů**

Chcete-li povolit kontrolu zabezpečení pro příkazy, přidejte profily do třídy MQCMDS. Názvy profilů jsou založeny na příkazech MQSC, ale kontrolují příkazy MQSC a PCF. Profily lze použít pro správce front nebo skupinu sdílení front.

Chcete-li zkontrolovat zabezpečení příkazů (takže jste nedefinovali profil přepínačů zabezpečení příkazu hlq.NO.COMD.CHECKS), musíte přidat profily do třídy MQCMDS.

Tytéž profily zabezpečení řídí příkazy MQSC a PCF. Názvy profilů produktu RACF pro kontrolu zabezpečení příkazů jsou založeny na názvech příkazů MQSC. Tyto profily mají formu:

```
hlq.verb.pkw
```

Kde hlq může být buď qmgr - name (název správce front) nebo qsg - name (název skupiny sdílení front), verb je sloveso část názvu příkazu, například ALTER, a pkw je typ objektu, například QLOCAL pro lokální frontu.

Proto je název profilu pro příkaz ALTER QLOCAL v subsystému CSQ1 následující:

```
CSQ1.ALTER.QLOCAL
```

Generické profily můžete použít k ochraně sad příkazů tak, abyste měli méně profilů k údržbě, a tedy méně seznamů pro přístup. Zvažte vytvoření generického profilu, který platí pro všechny příkazy, které nejsou chráněné specifitěji profilem. Definujte tento profil pomocí UACC (NONE) a udělte přístup ALTER pouze ke skupinám RACF, které obsahují administrátory. Pak můžete vytvořit generický profil použitelný pro všechny příkazy DISPLAY a udělit rozšířený přístup k němu. Mezi těmito extrémly můžete identifikovat skupiny uživatelů, kteří potřebují přístup k určitým sadám příkazů. V takovém případě můžete vytvářet profily pro tyto sady a udělit přístup skupinám uživatelů RACF zastupujícím tyto třídy uživatelů. Vyhněte

se tomu, aby uživatelé měli přístup k příkazům, které nevyžadují: Použijte zásadu alespoň oprávnění, aby měli uživatelé přístup pouze k příkazům, které jsou vyžadovány pro jejich úlohy.

Profil s předponou názvu správce front řídí použití tohoto příkazu v daném správci front. Profil s předponou názvu skupiny sdílení front řídí použití tohoto příkazu ve všech správcích front v rámci skupiny sdílení front. Tento přístup lze u jednotlivých správců front potlačit definováním profilu úrovně správce front pro daný příkaz v daném správci front.

Je-li váš správce front členem skupiny sdílení front a používáte-li správce front i zabezpečení na úrovni skupiny sdílení front, produkt IBM MQ vyhledá předponu s předponou názvu správce front. Pokud ji nenajde, hledá profil s předponou název skupiny sdílení front.

Nastavením profilů příkazů na úrovni správce front může být uživatel omezen na vydávání příkazů v konkrétním správci front. Případně můžete definovat jeden profil pro skupinu sdílení front pro každé příkazové slovo a všechny kontroly zabezpečení se místo jednotlivých správců front budou provádět s tímto profilem.

Je-li zabezpečení subsystému i zabezpečení skupiny sdílení front aktivní a lokální profil nebyl nalezen, provede se kontrola zabezpečení příkazu, aby se zjistilo, zda má uživatel přístup k profilu skupiny sdílení front.

Pokud použijete atribut CMDSCOPE pro směrování příkazu do jiných správců front ve skupině sdílení front, zkontroluje se zabezpečení každého správce front, ve kterém je příkaz spuštěn, ale nemusí být nutně ve správci front, ve kterém je zadán příkaz.

Tabulka 47 na stránce 205 zobrazuje pro každý příkaz IBM MQ MQSC profily vyžadované pro kontrolu zabezpečení příkazu a odpovídající úroveň přístupu pro každý profil ve třídě MQCMDS.

Tabulka 48 na stránce 212 zobrazuje pro každý příkaz IBM MQ PCF profily nezbytné pro kontrolu zabezpečení příkazů a odpovídající úroveň přístupu pro každý profil ve třídě MQCMDS.

Příkaz	Profil příkazu pro MQCMDS	Úroveň přístupu pro MQCMDS	Profil prostředků příkazů pro MQADMIN nebo MXADMIN	Úroveň přístupu pro MQADMIN nebo MXADMIN
ZMĚNIT AUTHINFO	hlq.ALTER.AUTHINFO	ALTER	hlq.AUTHINFO.resourcenam e	ALTER
ZMĚNIT FOND VYROVNÁVACÍCH PAMĚTÍ	hlq.ALTER.BUFFPOOL	ALTER	Žádná kontrola	-
ZMĚNIT CFSTRUCT	hlq.ALTER.CFSTRUCT	ALTER	Žádná kontrola	-
ZMĚNIT KANÁL	hlq.ALTER.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
ZMĚNIT SEZNAM NÁZVŮ	hlq.ALTER.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
ZMĚNIT PROCES	hlq.ALTER.PROCESS	ALTER	hlq.PROCESS.process	ALTER
POZMĚNIT PSID	hlq.ALTER.PSID	ALTER	Žádná kontrola	-
ZMĚNIT ALIAS QALIAS	hlq.ALTER.QALIAS	ALTER	hlq.QUEUE.queue	ALTER
POZMĚNIT QLOCAL	hlq.ALTER.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
ZMĚNIT QMGR	hlq.ALTER.QMGR	ALTER	Žádná kontrola	-

Tabulka 47. Příkazy MQSC, profily a jejich úrovně přístupu (pokračování)

Příkaz	Profil příkazu pro MQCMDS	Úroveň přístupu pro MQCMDS	Profil prostředků příkazů pro MQADMIN nebo MXADMIN	Úroveň přístupu pro MQADMIN nebo MXADMIN
ZMĚNIT MODEL QMODEL	hlq.ALTER.QMODEL	ALTER	hlq.QUEUE.queue	ALTER
ZMĚNIT QREMOTE	hlq.ALTER.QREMOTE	ALTER	hlq.QUEUE.queue	ALTER
POZMĚNIT ZABEZPEČENÍ	hlq.ALTER.SECURITY	ALTER	Žádná kontrola	-
POZMĚNIT SMDS	hlq.ALTER.SMDS	ALTER	Žádná kontrola	-
ZMĚNIT TŘÍDU STGCLASS	hlq.ALTER.STGCLASS	ALTER	Žádná kontrola	-
ZMĚNIT DÍLČÍ	hlq.ALTER.SUB	ALTER	Žádná kontrola	-
ALTER TOPIC	hlq.ALTER.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
ZMĚNIT TRASOVÁNÍ	hlq.ALTER.TRACE	ALTER	Žádná kontrola	-
PROTOKOL ARCHIVACE	hlq.ARCHIVE.LOG	CONTROL	Žádná kontrola	-
ZÁLOŽNÍ FSTRUCT	hlq.BACKUP.CFSTRUCT	CONTROL	Žádná kontrola	-
VYMAZAT QLOCAL	hlq.CLEAR.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
CLEAR TOPICSTR "3" <a href="#">na stránce 211</a>	hlq.CLEAR.TOPICSTR	ALTER	hlq.TOPIC.topic	ALTER
DEFINOVAT AUTHINFO	hlq.DEFINE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcenam e	ALTER
DEFINOVAT FOND VYROVNÁVACÍCH PAMĚTÍ	hlq.DEFINE.BUFFPOOL	ALTER	Žádná kontrola	-
DEFINOVAT CFSTRUCT	hlq.DEFINE.CFSTRUCT	ALTER	Žádná kontrola	-
Definovat kanál	hlq.DEFINE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
DEFINOVAT PROTOKOL	hlq.DEFINE.LOG	ALTER	Žádná kontrola	-
DEFINOVAT HODNOTY MAXSMSGS	hlq.DEFINE.MAXSMSGS	ALTER	Žádná kontrola	-
DEFINOVAT SEZNAM NÁZVŮ	hlq.DEFINE.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
DEFINOVÁNÍ PROCESU	hlq.DEFINE.PROCESS	ALTER	hlq.PROCESS.process	ALTER
DEFINOVAT PSID	hlq.DEFINE.PSID	ALTER	Žádná kontrola	-
DEFINOVAT ALIAS QALIAS	hlq.DEFINE.QALIAS	ALTER	hlq.QUEUE.queue	ALTER

Tabulka 47. Příkazy MQSC, profily a jejich úrovně přístupu (pokračování)

Příkaz	Profil příkazu pro MQCMDS	Úroveň přístupu pro MQCMDS	Profil prostředků příkazů pro MQADMIN nebo MXADMIN	Úroveň přístupu pro MQADMIN nebo MXADMIN
DEFINOVAT QLOCAL	hlq.DEFINE.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
DEFINOVAT MODEL QMODEL	hlq.DEFINE.QMODEL	ALTER	hlq.QUEUE.queue	ALTER
DEFINOVAT QREMOTE	hlq.DEFINE.QREMOTE	ALTER	hlq.QUEUE.queue	ALTER
DEFINOVAT TŘÍDU STGCLASS	hlq.DEFINE.STGCLASS	ALTER	Žádná kontrola	-
DEFINE SUB	hlq.DEFINE.SUB	ALTER	Žádná kontrola	-
DEFINOVAT TÉMA	hlq.DEFINE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
ODSTRANIT AUTHINFO	hlq.DELETE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcenam e	ALTER
ODSTRANIT FOND VYROVNÁVACÍCH PAMĚTÍ	hlq.DELETE.BUFFPOOL	ALTER	Žádná kontrola	-
ODSTRANIT CFSTRUCT	hlq.DELETE.CFSTRUCT	ALTER	Žádná kontrola	-
Odstranit kanál	hlq.DELETE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
Odstranit seznam názvů	hlq.DELETE.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
Odstranit proces	hlq.DELETE.PROCESS	ALTER	hlq.PROCESS.process	ALTER
ODSTRANIT PSID	hlq.DELETE.PSID	ALTER	Žádná kontrola	-
ODSTRANIT ALIAS QALIAS	hlq.DELETE.QALIAS	ALTER	hlq.QUEUE.queue	ALTER
ODSTRANIT QLOCAL	hlq.DELETE.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
ODSTRANIT MODEL QMODEL	hlq.DELETE.QMODEL	ALTER	hlq.QUEUE.queue	ALTER
ODSTRANIT QREMOTE	hlq.DELETE.QREMOTE	ALTER	hlq.QUEUE.queue	ALTER
ODSTRANIT STGCLASS	hlq.DELETE.STGCLASS	ALTER	Žádná kontrola	-
ODSTRANIT DÍLČÍ	hlq.DELETE.SUB	ALTER	Žádná kontrola	-
Odstranit téma	hlq.DELETE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
<a href="#">“1” na stránce 211 ARCHIVACE</a>	hlq.DISPLAY.ARCHIVE	READ (čtení)	Žádná kontrola	-
ZOBRAZIT AUTHINFO	hlq.DISPLAY.AUTHINFO	READ (čtení)	Žádná kontrola	-

Tabulka 47. Příkazy MQSC, profily a jejich úrovně přístupu (pokračování)

<b>Příkaz</b>	<b>Profil příkazu pro MQCMDS</b>	<b>Úroveň přístupu pro MQCMDS</b>	<b>Profil prostředků příkazů pro MQADMIN nebo MXADMIN</b>	<b>Úroveň přístupu pro MQADMIN nebo MXADMIN</b>
ZOBRAZIT STAV CFSTATUS	hlq.DISPLAY.CFSTATUS	READ (čtení)	Žádná kontrola	-
ZOBRAZIT CFSTRUCT	hlq.DISPLAY.CFSTRUCT	READ (čtení)	Žádná kontrola	-
ZOBRAZIT KANÁL	hlq.DISPLAY.CHANNEL	READ (čtení)	Žádná kontrola	-
ZOBRAZIT CHINIT	hlq.DISPLAY.CHINIT	READ (čtení)	Žádná kontrola	-
ZOBRAZIT VELIKOST CHUSH	hlq.DISPLAY.CHLAUTH	READ (čtení)	Žádná kontrola	-
ZOBRAZIT STAV CHSTATUS	hlq.DISPLAY.CHSTATUS	READ (čtení)	Žádná kontrola	-
ZOBRAZIT CLUQMGR	hlq.DISPLAY.CLUSQMGR	READ (čtení)	Žádná kontrola	-
ZOBRAZIT CMDSERV	hlq.DISPLAY.CMDSERV	READ (čtení)	Žádná kontrola	-
DISPLAY CONN "1" na <a href="#">stránce 211</a>	hlq.DISPLAY.CONN	READ (čtení)	Žádná kontrola	-
Zobrazit skupinu	hlq.DISPLAY.GROUP	READ (čtení)	Žádná kontrola	-
DISPLAY LOG "1" na <a href="#">stránce 211</a>	hlq.DISPLAY.LOG	READ (čtení)	Žádná kontrola	-
ZOBRAZIT VLASTNOSTI MAXSMSGS	hlq.DISPLAY.MAXSMSGS	READ (čtení)	Žádná kontrola	-
ZOBRAZIT SEZNAM NÁZVŮ	hlq.DISPLAY.NAMELIST	READ (čtení)	Žádná kontrola	-
ZOBRAZIT PROCES	hlq.DISPLAY.PROCESS	READ (čtení)	Žádná kontrola	-
ZOBRAZIT PUBSUB	hlq.DISPLAY.PUBSUB	READ (čtení)	Žádná kontrola	-
ZOBRAZIT ALIAS QALIAS	hlq.DISPLAY.QALIAS	READ (čtení)	Žádná kontrola	-
ZOBRAZIT QCLUSTER	hlq.DISPLAY.QCLUSTER	READ (čtení)	Žádná kontrola	-
ZOBRAZIT QLOCAL	hlq.DISPLAY.QLOCAL	READ (čtení)	Žádná kontrola	-

Tabulka 47. Příkazy MQSC, profily a jejich úrovně přístupu (pokračování)

Příkaz	Profil příkazu pro MQCMDS	Úroveň přístupu pro MQCMDS	Profil prostředků příkazů pro MQADMIN nebo MXADMIN	Úroveň přístupu pro MQADMIN nebo MXADMIN
ZOBRAZIT QMGR	hlq.DISPLAY.QMGR	READ (čtení)	Žádná kontrola	-
ZOBRAZIT MODEL QMODEL	hlq.DISPLAY.QMODEL	READ (čtení)	Žádná kontrola	-
ZOBRAZIT QREMOTE	hlq.DISPLAY.QREMOTE	READ (čtení)	Žádná kontrola	-
ZOBRAZIT STAV QSTATUS	hlq.DISPLAY.QSTATUS	READ (čtení)	Žádná kontrola	-
ZOBRAZIT FRONTU	hlq.DISPLAY.QUEUE	READ (čtení)	Žádná kontrola	-
ZOBRAZIT STAV SBSTATUS	hlq.DISPLAY.SBSTATUS	READ (čtení)	Žádná kontrola	-
Zobrazit sadu SMDS	hlq.DISPLAY.SMDS	READ (čtení)	Žádná kontrola	-
ZOBRAZIT PŘIPOJENÍ SMDSCONN	hlq.DISPLAY.SMDSCONN	READ (čtení)	Žádná kontrola	-
ZOBRAZIT POD	hlq.DISPLAY.SUB	READ (čtení)	Žádná kontrola	-
ZOBRAZIT ZABEZPEČENÍ	hlq.DISPLAY.SECURITY	READ (čtení)	Žádná kontrola	-
ZOBRAZIT TŘÍDU STGCLASS	hlq.DISPLAY.STGCLASS	READ (čtení)	Žádná kontrola	-
SYSTÉM DISPLAY <a href="#">“1” na stránce 211</a>	hlq.DISPLAY.SYSTEM	READ (čtení)	Žádná kontrola	-
ZOBRAZIT VLÁKNO	hlq.DISPLAY.THREAD	READ (čtení)	Žádná kontrola	-
ZOBRAZIT STAV TPSTATUS	hlq.DISPLAY.TPSTATUS	READ (čtení)	Žádná kontrola	-
ZOBRAZIT TÉMA	hlq.DISPLAY.TOPIC	READ (čtení)	Žádná kontrola	-
ZOBRAZIT STAV TPSTATUS	hlq.DISPLAY.TPSTATUS	READ (čtení)	Žádná kontrola	-
ZOBRAZIT TRASOVÁNÍ	hlq.DISPLAY.TRACE	READ (čtení)	Žádná kontrola	-
Zobrazení využití <a href="#">“1” na stránce 211</a>	hlq.DISPLAY.USAGE	READ (čtení)	Žádná kontrola	-
PŘESUNOUT QLOCAL	hlq.MOVE.QLOCAL	ALTER	hlq.QUEUE.from-queue hlq.QUEUE.to-queue	ALTER

Tabulka 47. Příkazy MQSC, profily a jejich úrovně přístupu (pokračování)

Příkaz	Profil příkazu pro MQCMDS	Úroveň přístupu pro MQCMDS	Profil prostředků příkazů pro MQADMIN nebo MXADMIN	Úroveň přístupu pro MQADMIN nebo MXADMIN
Odeslat signál Ping pro kanál	hlq.PING.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Obnovit BSDS	hlq.RECOVER.BSDS	CONTROL	Žádná kontrola	-
OBNOVIT CFSTRUCT	hlq.RECOVER.CFSTRUCT	CONTROL	Žádná kontrola	-
Aktualizovat klastr	hlq.REFRESH.CLUSTER	ALTER	Žádná kontrola	-
AKTUALIZOVAT SPRÁVCE FRONT	hlq.REFRESH.QMGR	ALTER	Žádná kontrola	-
REFRESH SECURITY	hlq.REFRESH.SECURITY	ALTER	Žádná kontrola	-
RESETOVAT CFSTRUCT	hlq.RESET.CFSTRUCT	CONTROL	Žádná kontrola	-
Resetovat kanál	hlq.RESET.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Reset klastru	hlq.RESET.CLUSTER	CONTROL	Žádná kontrola	-
RESETOVAT QMGR	hlq.RESET.QMGR	CONTROL	Žádná kontrola	-
RESETOVAT QSTATS	hlq.RESET.QSTATS	CONTROL	hlq.QUEUE.queue	CONTROL
Resetovat SMDS	hlq.RESET.SMDS	CONTROL	Žádná kontrola	-
Obnovit položku Tpipe	hlq.RESET.TPIPE	CONTROL	Žádná kontrola	-
Vyřešit kanál	hlq.RESOLVE.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Vyřešit nejisté položky	hlq.RESOLVE.INDOUBT	CONTROL	Žádná kontrola	-
OBNOVIT SPRÁVCE FRONT	hlq.RESUME.QMGR	CONTROL	Žádná kontrola	-
ZABEZPEČENÍ OVĚŘENÍ	hlq.RVERIFY.SECURITY	ALTER	Žádná kontrola	-
Nastavit archiv	hlq.SET.ARCHIVE	CONTROL	Žádná kontrola	-
SET CHLAUTH	hlq.SET.CHLAUTH	CONTROL	Žádná kontrola	-
Nastavit protokol	hlq.SET.LOG	CONTROL	Žádná kontrola	-
Nastavit systém	hlq.SET.SYSTEM	CONTROL	Žádná kontrola	-
Spustit kanál	hlq.START.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
START CHINIT "4" na stránce 211	hlq.START.CHINIT	CONTROL	Žádná kontrola	-
SPUSTIT CMDSERV	hlq.START.CMDSERV	CONTROL	Žádná kontrola	-
Spustit listener	hlq.START.LISTENER	CONTROL	Žádná kontrola	-
SPUSTIT SPRÁVCE FRONT	Není "2" na stránce 211	-	-	-

Tabulka 47. Příkazy MQSC, profily a jejich úrovně přístupu (pokračování)

Příkaz	Profil příkazu pro MQCMDS	Úroveň přístupu pro MQCMDS	Profil prostředků příkazů pro MQADMIN nebo MXADMIN	Úroveň přístupu pro MQADMIN nebo MXADMIN
SPUSTIT PŘÍKAZ SMDSCONN	hlq.START.SMDSCONN	CONTROL	Žádná kontrola	-
Spustit trasování	hlq.START.TRACE	CONTROL	Žádná kontrola	-
Ukončit kanál	hlq.STOP.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
UKONČIT CHINIT	hlq.STOP.CHINIT	CONTROL	Žádná kontrola	-
UKONČIT CMDSERV	hlq.STOP.CMDSERV	CONTROL	Žádná kontrola	-
Ukončit listener	hlq.STOP.LISTENER	CONTROL	Žádná kontrola	-
ZASTAVIT QMGR	hlq.STOP.QMGR	CONTROL	Žádná kontrola	-
ZASTAVIT PŘÍKAZ SMDSCONN	hlq.STOP.SMDSCONN	CONTROL	Žádná kontrola	-
Zastavit trasování	hlq.STOP.TRACE	CONTROL	Žádná kontrola	-
SUSPEND QMgr	hlq.SUSPEND.QMGR	CONTROL	Žádná kontrola	-

**Notes:**

1. Tyto příkazy mohou být vydávány interně správcem front; v těchto případech se nekontroluje žádná oprávnění.
2. IBM MQ nekontroluje oprávnění uživatele, který vydává příkaz START QMGR. Můžete však použít produkt RACF nebo alternativní zařízení zabezpečení k řízení přístupu k příkazu START xxxxMSTR, který je vydán jako výsledek příkazu START QMGR. To se provádí řízením přístupu k profilu MVS.START.STC.xxxxMSTR ve třídě operátorů operátorů RACF (OPERCMD5). Podrobné informace o této proceduře naleznete v příručce *z/OS SecureWay Security Server RACF Security Administrator's Guide*. Použijete-li tuto techniku a neautorizovaný uživatel se pokusí spustit správce front, bude ukončen s kódem příčiny 00F30216.
3. Prostředek **hlq.TOPIC.topic** se odkazuje na objekt Topic odvozený z TOPCSTR. Další informace viz ["Zabezpečení publikování/odběru"](#) na stránce 410
4. Ve vydáních před verzí IBM MQ for z/OS V6 byla kontrola zabezpečení pro MVS.START.STC.CSQ1CHIN. Ve verzi IBM MQ for z/OS V6 a vyšší má k názvu prostředku k sobě přidán další kvalifikátor JOBNAME. To může způsobit problémy při spouštění inicializátoru kanálu.

Chcete-li vyřešit problém, nahradte MVS.START.STC. ssid CHIN s profilem pro prostředek s názvem MVS.START.STC. ssid CHIN.\* nebo MVS.START.STC. ssid CHIN. ssid CHIN, kde ssid je ID subsystému pro správce front. To vyžaduje oprávnění RACF UPDATE. Další podrobnosti viz [Dokumentace produktu z/OS pro Plánování operací, Příkazy MVS, přístupové autority RACF a názvy prostředků](#).

Příkaz START pro ssid MSTR nezahrnuje parametr JOBNAME=. V zájmu konzistence možná budete chtít aktualizovat profil pro MVS.START.STC.ssidMSTR na MVS.START.STC.ssidMSTR.\*



Tabulka 48. PCF příkazy, profily a jejich úroveň přístupu

Příkaz	Profil příkazu pro MQCMD5	Úroveň přístupu pro MQCMD5	Profil prostředků příkazů pro MQADMIN nebo MXADMIN	Úroveň přístupu pro MQADMIN nebo MXADMIN
Zálohovat strukturu CF	hlq.BACKUP.CFSTRUCT	CONTROL	Žádná kontrola	-
Změnit objekt ověřovacích informací	hlq.ALTER.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
Změnit strukturu CF	hlq.ALTER.CFSTRUCT	ALTER	Žádná kontrola	-
Změnit kanál	hlq.ALTER.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
Změnit seznam názvů	hlq.ALTER.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
Změnit proces	hlq.ALTER.PROCESS	ALTER	hlq.PROCESS.process	ALTER
Změnit frontu	hlq.ALTER.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
Změnit správce front	hlq.ALTER.QMGR	ALTER	Žádná kontrola	-
Změna zabezpečení	hlq.ALTER.SECURITY	ALTER	Žádná kontrola	-
Změnit SMDS	hlq.ALTER.SMDS	ALTER	Žádná kontrola	-
Změnit úložnou třídu	hlq.ALTER.STGCLASS	ALTER	Žádná kontrola	-
Změnit odběr	hlq.ALTER.SUB	ALTER	Žádná kontrola	-
Změnit téma	hlq.ALTER.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
Vymazat frontu	hlq.CLEAR.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
Vymazat řetězec tématu "1" na stránce 215	hlq.CLEAR.TOPICSTR	ALTER	hlq.TOPIC.topic	ALTER
Kopírování objektu ověřovacích informací	hlq.DEFINE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
Kopírovat strukturu CF	hlq.DEFINE.CFSTRUCT	ALTER	Žádná kontrola	-
Kopírovat kanál	hlq.DEFINE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
Kopírovat seznam názvů	hlq.DEFINE.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
Kopírovat proces	hlq.DEFINE.PROCESS	ALTER	hlq.PROCESS.process	ALTER
Kopírovat frontu	hlq.DEFINE.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
Kopírovat odběr	hlq.DEFINE.SUB	ALTER	Žádná kontrola	-
Kopírovat úložnou třídu	hlq.DEFINE.STGCLASS	ALTER	Žádná kontrola	-
Kopírovat téma	hlq.DEFINE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
Vytvořit objekt ověřovacích informací	hlq.DEFINE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
Vytvořit strukturu CF	hlq.DEFINE.CFSTRUCT	ALTER	Žádná kontrola	-
Vytvořit kanál	hlq.DEFINE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
Vytvořit seznam názvů	hlq.DEFINE.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
Vytvořit proces	hlq.DEFINE.PROCESS	ALTER	hlq.PROCESS.process	ALTER
Vytvořit frontu	hlq.DEFINE.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
Vytvořit úložnou třídu	hlq.DEFINE.STGCLASS	ALTER	Žádná kontrola	-

Tabulka 48. PCF příkazy, profily a jejich úroveň přístupu (pokračování)

<b>Příkaz</b>	<b>Profil příkazu pro MQCMDS</b>	<b>Úroveň přístupu pro MQCMDS</b>	<b>Profil prostředků příkazů pro MQADMIN nebo MXADMIN</b>	<b>Úroveň přístupu pro MQADMIN nebo MXADMIN</b>
Vytvořit odběr	hlq.DEFINE.SUB	ALTER	Žádná kontrola	-
Vytvořit téma	hlq.DEFINE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
Odstranit objekt ověřovacích informací	hlq.DELETE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
Odstranit strukturu CF	hlq.DELETE.CFSTRUCT	ALTER	Žádná kontrola	-
Odstranit kanál	hlq.DELETE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
Odstranit seznam názvů	hlq.DELETE.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
Odstranit proces	hlq.DELETE.PROCESS	ALTER	hlq.PROCESS.process	ALTER
Odstranit frontu	hlq.DELETE.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
Odstranit úložnou třídu	hlq.DELETE.STGCLASS	ALTER	Žádná kontrola	-
Odstranit odběr	hlq.DELETE.SUB	ALTER	Žádná kontrola	-
Odstranit téma	hlq.DELETE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
Zjistit archiv	hlq.DISPLAY.ARCHIVE	READ (čtení)	Žádná kontrola	-
Zjistit objekt ověřovacích informací	hlq.DISPLAY.AUTHINFO	READ (čtení)	Žádná kontrola	-
Zjišťovat názvy objektů ověřovacích informací	hlq.DISPLAY.AUTHINFO	READ (čtení)	Žádná kontrola	-
Zjistit strukturu CF	hlq.DISPLAY.CFSTRUCT	READ (čtení)	Žádná kontrola	-
Zjistit názvy struktury CF	hlq.DISPLAY.CFSTRUCT	READ (čtení)	Žádná kontrola	-
Zjistit stav struktury CF	hlq.DISPLAY.CFSTATUS	READ (čtení)	Žádná kontrola	-
Zjistit kanál	hlq.DISPLAY.CHANNEL	READ (čtení)	Žádná kontrola	-
Zjistit záznam ověření kanálu	hlq.DISPLAY.CHLAUTH	READ (čtení)	Žádná kontrola	-
Zjistit inicializátor kanálu	hlq.DISPLAY.CHINIT	READ (čtení)	Žádná kontrola	-
Zjistit názvy kanálů	hlq.DISPLAY.CHANNEL	READ (čtení)	Žádná kontrola	-
Zjistit stav kanálu	hlq.DISPLAY.CHSTATUS	READ (čtení)	Žádná kontrola	-
Zjistit správce front klastru	hlq.DISPLAY.CLUSQMGR	READ (čtení)	Žádná kontrola	-
Zjistit připojení	hlq.DISPLAY.CONNPCF	READ (čtení)	Žádná kontrola	-
Zjišťovat skupinu	hlq.DISPLAY.GROUP	READ (čtení)	Žádná kontrola	-
Zjistit protokol	hlq.DISPLAY.LOG	READ (čtení)	Žádná kontrola	-
Zjistit seznam názvů	hlq.DISPLAY.NAMELIST	READ (čtení)	Žádná kontrola	-
Zjistit názvy seznamů názvů	hlq.DISPLAY.NAMELIST	READ (čtení)	Žádná kontrola	-
Zjistit proces	hlq.DISPLAY.PROCESS	READ (čtení)	Žádná kontrola	-
Zjistit názvy procesů	hlq.DISPLAY.PROCESS	READ (čtení)	Žádná kontrola	-

Tabulka 48. PCF příkazy, profily a jejich úroveň přístupu (pokračování)

<b>Příkaz</b>	<b>Profil příkazu pro MQCMDS</b>	<b>Úroveň přístupu pro MQCMDS</b>	<b>Profil prostředků příkazů pro MQADMIN nebo MXADMIN</b>	<b>Úroveň přístupu pro MQADMIN nebo MXADMIN</b>
Zjistit stav publikování/ odběru	hlq.DISPLAY.PUBSUB	READ (čtení)	Žádná kontrola	-
Zjistit frontu	hlq.DISPLAY.QUEUE	READ (čtení)	Žádná kontrola	-
Zjistit správce front	hlq.DISPLAY.QMGR	READ (čtení)	Žádná kontrola	-
Zjistit názvy front	hlq.DISPLAY.QUEUE	READ (čtení)	Žádná kontrola	-
Zjistit stav fronty	hlq.DISPLAY.QSTATUS	READ (čtení)	Žádná kontrola	-
Zjistit zabezpečení	hlq.DISPLAY.SECURITY	READ (čtení)	Žádná kontrola	-
Zjistit SMDS	hlq.DISPLAY.SMDS	READ (čtení)	Žádná kontrola	-
Zjistit SMDSCONN	hlq.DISPLAY.SMDSCONN	READ (čtení)	Žádná kontrola	-
Zjistit úložnou třídu	hlq.DISPLAY.STGCLASS	READ (čtení)	Žádná kontrola	-
Zjistit názvy úložné třídy	hlq.DISPLAY.STGCLASS	READ (čtení)	Žádná kontrola	-
Zjistit odběr	hlq.INQUIRE.SUB	READ (čtení)	Žádná kontrola	-
Zjistit stav odběru	hlq.INQUIRE.SBSTATUS	READ (čtení)	Žádná kontrola	-
Zjistit systém	hlq.DISPLAY.SYSTEM	READ (čtení)	Žádná kontrola	-
Zjistit téma	hlq.DISPLAY.TOPIC	READ (čtení)	Žádná kontrola	-
Zjistit názvy témat	hlq.DISPLAY.TOPIC	READ (čtení)	Žádná kontrola	-
Zjistit stav tématu	hlq.DISPLAY.TPSTATUS	READ (čtení)	Žádná kontrola	-
Zjistit použití	hlq.DISPLAY.USAGE	READ (čtení)	Žádná kontrola	-
Přesunout frontu	hlq.MOVE.QLOCAL	ALTER	hlq.QUEUE.from-queue hlq.QUEUE.to-queue	ALTER
Odeslat signál Ping pro kanál	hlq.PING.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Obnovit strukturu CF	hlq.RECOVER.CFSTRUCT	CONTROL	Žádná kontrola	-
Aktualizovat klastr	hlq.REFRESH.CLUSTER	ALTER	Žádná kontrola	-
Aktualizovat správce front	hlq.REFRESH.QMGR	ALTER	Žádná kontrola	-
Aktualizovat zabezpečení	hlq.REFRESH.SECURITY	ALTER	Žádná kontrola	-
Resetovat strukturu CF	hlq.RESET.CFSTRUCT	CONTROL	Žádná kontrola	-
Resetovat kanál	hlq.RESET.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Reset klastru	hlq.RESET.CLUSTER	CONTROL	Žádná kontrola	-
Obnovit správce front	hlq.RESET.QMGR	CONTROL	Žádná kontrola	-
Obnovit statistiku front	hlq.RESET.QSTATS	CONTROL	hlq.QUEUE.queue	CONTROL
Resetovat SMDS	hlq.RESET.SMDS	CONTROL	Žádná kontrola	-
Vyřešit kanál	hlq.RESOLVE.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Obnovit správce front	hlq.RESUME.QMGR	CONTROL	Žádná kontrola	-

Tabulka 48. PCF příkazy, profily a jejich úroveň přístupu (pokračování)

Příkaz	Profil příkazu pro MQCMDS	Úroveň přístupu pro MQCMDS	Profil prostředků příkazů pro MQADMIN nebo MXADMIN	Úroveň přístupu pro MQADMIN nebo MXADMIN
Obnovit klastr správců front	hlq.RESUME.QMGR	CONTROL	Žádná kontrola	-
Znovu ověřit zabezpečení	hlq.RVERIFY.SECURITY	ALTER	Žádná kontrola	-
Nastavit archiv	hlq.SET.ARCHIVE	CONTROL	Žádná kontrola	-
Nastavit záznam ověření kanálu	hlq.SET.CHLAUTH	CONTROL	Žádná kontrola	-
Nastavit protokol	hlq.SET.LOG	CONTROL	Žádná kontrola	-
Nastavit systém	hlq.SET.SYSTEM	CONTROL	Žádná kontrola	-
Spustit kanál	hlq.START.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Spustit inicializátor kanálu	hlq.START.CHINIT	CONTROL	Žádná kontrola	-
Spustit modul listener kanálu	hlq.START.LISTENER	CONTROL	Žádná kontrola	-
Spustit připojení SMDS	hlq.START.SMDSCONN	CONTROL	Žádná kontrola	-
Ukončit kanál	hlq.STOP.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Ukončit inicializátor kanálu	hlq.STOP.CHINIT	CONTROL	Žádná kontrola	-
Zastavit modul listener kanálu	hlq.STOP.LISTENER	CONTROL	Žádná kontrola	-
Zastavit připojení SMDS	hlq.STOP.SMDSCONN	CONTROL	Žádná kontrola	-
Pozastavit správce front	hlq.SUSPEND.QMGR	CONTROL	Žádná kontrola	-
Pozastavit klastr správců front	hlq.SUSPEND.QMGR	CONTROL	Žádná kontrola	-

#### Notes:

1. Prostředek **hlq.TOPIC.topic** se odkazuje na objekt Topic odvozený z TOPCSTR. Další informace viz ["Zabezpečení publikování/odběru"](#) na stránce 410

#### **Profily pro zabezpečení prostředků příkazů**

Pokud jste nedefinovali profil přepínače zabezpečení prostředků příkazu, protože chcete kontrolu zabezpečení pro prostředky přidružené k příkazům, musíte přidat profily prostředků pro každý prostředek do příslušné třídy. Tytéž profily zabezpečení řídí příkazy MQSC a PCF.

Pokud jste nedefinovali profil přepínače zabezpečení prostředků příkazů, hlq.NO.CMD.RESC.CHECKS, protože chcete kontrolu zabezpečení pro prostředky přidružené k příkazům, musíte:

- Přidejte profil prostředku ve třídě **MQADMIN**, pokud používáte velké profily, pro každý prostředek.
- Přidejte profil prostředku ve třídě **MXADMIN**, pokud používáte pro každý prostředek kombinované profily případu.

Tytéž profily zabezpečení řídí příkazy MQSC a PCF.

Profily pro kontrolu zabezpečení prostředků příkazů mají formát:

```
hlq.type.resourcename
```

kde hlq může být buď qmgr-name (název správce front), nebo qsg-name (název skupiny sdílení front).

Profil s předponou názvu správce front řídí přístup k prostředkům přidruženým k příkazům v daném správci front. Profil s předponou názvu skupiny sdílení front řídí přístup k prostředkům přidruženým k příkazům ve všech správcích front v rámci skupiny sdílení front. Tento přístup lze u jednotlivých správců front potlačit definováním profilu úrovně správce front pro daný prostředek příkazu v daném správci front.


Je-li váš správce front členem skupiny sdílení front a používáte-li správce front i zabezpečení na úrovni skupiny sdílení front, produkt IBM MQ nejprve zkontroluje profil s předponou názvu správce front. Pokud jej nenajde, hledá profil s předponou názvu skupiny sdílení front.


Například název profilu produktu RACF pro kontrolu zabezpečení prostředků příkazů ve vztahu k modelové frontě CREDIT.WORTHY v podsystému CSQ1 je:

```
CSQ1.QUEUE.CREDIT.WORTHY
```

Vzhledem k tomu, že profily pro všechny typy příkazových prostředků jsou umístěny ve třídě MQADMIN, je v profilu zapotřebí část "type" profilu pro rozlišení mezi prostředky různých typů, které mají stejný název. Část názvu profilu "type" může být CHANNEL, QUEUE, TOPIC, PROCESS nebo NAMELIST. Uživatel může být například oprávněn definovat hlq.QUEUE.PAYROLL.ONE, ale nemáte autorizaci k definování hlq.PROCESS.PAYROLL.ONE

Je-li typem prostředku fronta a profil je profil na úrovni skupiny sdílení front, řídí přístup k jedné nebo více lokálním frontám v rámci skupiny sdílení front, nebo přístup k jedné sdílené frontě z libovolného správce front v rámci skupiny sdílení front.

 Příkazy MQSC, profily a jejich úrovně přístupu ukazují pro každý příkaz IBM MQ MQSC, profily nezbytné pro kontrolu zabezpečení příkazů a odpovídající úroveň přístupu pro každý profil ve třídě MQCMDS.

 Příkazy PCF, profily a jejich úrovně přístupu zobrazují pro každý příkaz IBM MQ PCF profily nezbytné pro kontrolu zabezpečení příkazů a odpovídající úroveň přístupu pro jednotlivé profily ve třídě MQCMDS.

*Kontrola zabezpečení prostředků příkazů pro fronty aliasů a vzdálené fronty*

Fronta aliasů a vzdálené fronty poskytují přesměrování do jiné fronty. Další body se použijí, když zvážíte kontrolu zabezpečení pro tyto fronty.

## Alias fronty

Pokud definujete alias frontu, jsou kontroly zabezpečení prostředků příkazů prováděny pouze s názvem fronty aliasů, nikoli s názvem cílové fronty, na kterou je alias interpretováno.

Fronty aliasů se mohou interpretovat jak lokální, tak i vzdálené fronty. Nechcete-li uživatelům povolit přístup k určitým lokálním nebo vzdáleným frontám, musíte provést obě tyto akce:

1. Neumožněte uživatelům přístup k těmto lokálním a vzdáleným frontám.
2. Omezte uživatele tak, aby mohli definovat aliasy pro tyto fronty. To znamená, že zabráníte tomu, aby mohli vydávat příkazy DEFINE QALIAS a ALTER QALIAS.

## Vzdálené fronty

Když definujete vzdálenou frontu, jsou kontroly zabezpečení prostředků prováděny pouze proti názvu vzdálené fronty. Žádné kontroly se neprovádí proti názvům front uvedených v attributech RNAME nebo XMITQ v definici objektu vzdálené fronty.

## Profil zabezpečení RESLEVEL

Můžete definovat speciální profil ve třídě MQADMIN nebo MXADMIN k řízení počtu ID uživatelů kontrolovaných pro zabezpečení na úrovni rozhraní API. Tento profil se nazývá profil RESLEVEL. Způsob, jakým tento profil ovlivňuje zabezpečení na úrovni rozhraní API, závisí na tom, jak přistupujete k produktu IBM MQ.

Pokud se aplikace pokusí o připojení k produktu IBM MQ, produkt IBM MQ zkontroluje přístup, který má jméno uživatele přidružené k tomuto připojení k profilu ve třídě MQADMIN nebo MXADMIN s názvem:

```
hlq.RESLEVEL
```

Kde hlq může být buď ssid (ID subsystému), nebo qsg (ID skupiny sdílení front).

ID uživatele přidružená k jednotlivým typům připojení jsou:

- ID uživatele připojované úlohy pro dávkové připojení
- ID uživatele adresního prostoru CICS pro připojení CICS
- ID uživatele adresního prostoru IMS pro připojení IMS
- ID uživatele adresního prostoru iniciátoru kanálu pro připojení inicializátoru kanálu



**Upozornění:** RESLEVEL je velmi výkonná volba; může způsobit vynechání všech kontrol zabezpečení prostředků pro určité připojení.

Pokud nemáte definován profil RESLEVEL, musíte být opatrní, aby se žádný jiný profil ve třídě MQADMIN neshoduje s hlq.RESLEVEL. Máte-li například profil v MQADMIN s názvem hlq. \* \*, a žádný profil hlq.RESLEVEL, pozor na důsledky úlohy hlq. \* \* profil, protože se používá pro kontrolu RESLEVEL.

Definujte profil hlq.RESLEVEL a nastavte hodnotu UACC na hodnotu NONE, místo abyste žádný profil RESLEVEL vůbec nevytvořili. Je třeba mít co nejméně uživatelů nebo skupin v seznamu pro přístup. Podrobnosti o tom, jak auditovat přístup RESLEVEL, viz [“Aspekty auditování v systému z/OS”](#) na stránce 241.

Používáte-li pouze zabezpečení na úrovni správce front, produkt IBM MQ provádí kontroly RESLEVEL pro profil produktu qmgr-name.RESLEVEL. Používáte-li pouze zabezpečení na úrovni skupiny sdílení front, produkt IBM MQ provádí kontroly RESLEVEL pro profil produktu qsg-name.RESLEVEL. Používáte-li kombinaci zabezpečení na úrovni správce front i skupiny sdílení front, produkt IBM MQ nejprve zkontroluje existenci profilu RESLEVEL na úrovni správce front. Pokud ji nenajde, zkontroluje profil RESLEVEL na úrovni skupiny sdílení front.

Pokud nelze najít profil RESLEVEL, IBM MQ povoluje kontrolu úlohy a úlohy (nebo alternativního uživatele) pro připojení CICS nebo IMS. Pro dávkové připojení IBM MQ povoluje kontrolu ID uživatele úlohy (nebo alternativního) uživatele. Pro inicializátor kanálu umožňuje IBM MQ kontrolu ID uživatele kanálu a ID uživatele MCA (nebo alternativního).

Existuje-li profil RESLEVEL, úroveň kontroly závisí na úrovni prostředí a přístupu k profilu.

Pamatujte na to, že pokud je váš správce front členem skupiny sdílení front a nedefinujete tento profil na úrovni správce front, může existovat jedna definice na úrovni skupiny sdílení front, která bude mít vliv na úroveň checking.To aktivovat kontrolu dvou ID uživatelů, definujete profil RESLEVEL (s předponou s názvem správce front názvu skupiny sdílení front) s UACC (NONE) a ujistěte se, že příslušní uživatelé nemají přístup k tomuto profilu.

Když uvážíte přístup, který má ID uživatele iniciátoru kanálu k parametru RESLEVEL, nezapomeňte, že připojení ustanovené inicializačním programem kanálu je také připojení využívaným kanály. Nastavení, které způsobí vynechání všech kontrol zabezpečení prostředků pro ID uživatele iniciátoru kanálu efektivně obchází bezpečnostní kontroly pro všechny kanály. Je-li ID uživatele iniciátoru kanálu přístup k souboru RESLEVEL jiným než NONE, je pro přístup kontrolován pouze jedno ID uživatele (pro úroveň přístupu READ nebo UPDATE) nebo žádná ID uživatele (pro úroveň přístupu CONTROL nebo ALTER). Pokud přidělíte ID uživatele iniciátoru kanálu jinou úroveň přístupu než NONE, ujistěte se, že chápete vliv tohoto nastavení na kontroly zabezpečení prováděné pro kanály.

Použití profilu RESLEVEL znamená, že se neprovedou běžné záznamy auditu zabezpečení. Zadáte-li například UAUDIT na uživatele, přístup k profilu hlq.RESLEVEL v MQADMIN se nebude monitorovat.

Pokud použijete volbu WARNING produktu RACF v profilu hlq.RESLEVEL, nebudou pro profily ve třídě RESLEVEL vytvářeny žádné varovné zprávy produktu RACF.

Kontrola zabezpečení pro zprávy sestav, jako např. COD, je řízena profilem RESLEVEL přidruženým k původní aplikaci. Má-li například ID uživatele dávkové úlohy oprávnění CONTROL nebo ALTER pro profil RESLEVEL, bude vynechána kontrola všech prostředků provedených dávkovou úlohou, včetně kontroly zabezpečení zpráv sestav.

Změníte-li profil RESLEVEL, uživatelé se musí před změnou připojení znovu odpojit a znovu připojit. (To zahrnuje zastavení a restart inicializátoru kanálu, pokud je změněn přístup k ID uživatele distribuovaného adresního prostoru fronty do profilu RESLEVEL.)

Chcete-li vypnout auditování RESLEVEL, použijte parametr systému RESAUDIT.

### **RESLEVEL a dávková spojení**

Ve výchozím nastavení platí, že je-li k prostředku IBM MQ přístupován prostřednictvím dávkových a dávkových připojení, musí mít uživatel oprávnění k přístupu k danému prostředku pro konkrétní operaci. Kontrolováním zabezpečení můžete obejít kontrolu zabezpečení nastavením příslušné definice RESLEVEL.

Určuje, zda je uživatel kontrolován nebo není založen na ID uživatele použitém v době připojení, stejné ID uživatele použité pro kontrolu připojení.

Můžete například nastavit RESLEVEL tak, že když uživatel, kterému důvěřujete, přistupuje k určitým prostředkům prostřednictvím dávkového připojení, nejsou provedeny žádné kontroly zabezpečení prostředků API; ale když se uživatel, kterému nedůvěřuje, pokusí o přístup ke stejným prostředkům, kontroly zabezpečení se provedou jako normální. Kontrola RESLEVEL by měla být nastavena pouze tehdy, když jste dostatečně důvěřovali uživateli a programům, které spustil tento uživatel.

Následující tabulka zobrazuje kontroly provedené u dávkových připojení.

<b>RACF úroveň přístupu</b>	<b>Stupeň kontroly</b>
ŽÁDNÉ	Provedená kontrola prostředků
READ (čtení)	Provedená kontrola prostředků
AKTUALIZOVAT	Provedená kontrola prostředků
CONTROL	Žádná kontrola.
ALTER	Žádná kontrola.

### **RESLEVEL a systémové funkce**

Aplikace RESLEVEL pro operační a ovládací panely a pro CSQUTIL.

Ovládací panely a řídicí panely a obslužný program CSQUTIL jsou aplikace typu dávky, které vytvářejí požadavky na příkazový server správce front, a proto se vztahují na pokyny popsané v části “RESLEVEL a dávková spojení” na stránce 218. Můžete použít RESLEVEL k vynechání kontroly zabezpečení pro SYSTEM.COMMAND.INPUT a SYSTEM.COMMAND.REPLY.MODEL front, které používají, ale ne pro dynamické fronty SYSTEM.CSQXCMD. \*, SYSTEM.CSQOREXX.\*, a SYSTEM.CSQUTIL. \*.

Příkazový server je nedílnou součástí správce front, a proto k němu není přidružena žádná kontrola připojení nebo RESLEVEL. Chcete-li zachovat zabezpečení, musí proto příkazový server potvrdit, že ID uživatele žádající aplikace má oprávnění k otevření fronty používané pro odpovědi. Pro operace a ovládací panely je to SYSTEM.CSQOREXX. \*. Pro CSQUTIL je to SYSTEM.CSQUTIL. \*. Uživatelé musí mít oprávnění k používání těchto front, jak je popsáno v části “Zabezpečení systémové fronty” na stránce 191, a navíc k libovolné autorizaci RESLEVEL, která jsou jim udělena.

Pro ostatní aplikace používající příkazový server je to fronta, kterou pojmenujete jako jejich odpověď na frontu. Takové jiné aplikace mohou klamat příkazový server na umístování zpráv do neautorizovaných

front předáním (v kontextu zprávy) spolehlivějšího ID uživatele, než je jeho vlastní pro příkazový server. Chcete-li tomu zabránit, použijte profil CONTEXT k ochraně kontextu identity zpráv umístěných v systému SYSTEM.COMMAND.INPUT.

### **Připojení RESLEVEL a CICS**

Je-li při připojení k produktu CICS prováděna kontrola zabezpečení prostředků rozhraní API, je ve výchozím stavu zaškrtnuto dva ID uživatelů. Pomocí nastavení profilu RESLEVEL můžete změnit, která ID uživatele se kontrolují.

První ID uživatele bylo zkontrolováno, že je adresní prostor CICS . Jedná se o ID uživatele na zakázkový list úlohy CICS nebo ID uživatele přiřazeného ke spuštěné úloze CICS podle třídy z/OS STARTED nebo v tabulce spuštěných procedur. (Není to CICS DFLTUSER.)

Druhé kontrolované ID uživatele je ID uživatele přidružené k transakci CICS .

Pokud jedno z těchto ID uživatelů nemá přístup k prostředku, požadavek selže s kódem dokončení MQRC\_NOT\_AUTHORIZED. ID uživatele adresního prostoru CICS i ID uživatele, který spouští transakci produktu CICS , musí mít přístup k prostředku na správné úrovni.

### **Jak RESLEVEL může ovlivnit provedené kontroly**

V závislosti na tom, jak nastavíte profil RESLEVEL, můžete změnit, která ID uživatelů se kontrolují při požadavku na přístup k prostředku. Další informace viz [Tabulka 50 na stránce 219](#).

Kontrolovaná ID uživatelů závisí na ID uživatele použitým při připojení, to znamená, ID uživatele adresního prostoru CICS . Tento ovládací prvek vám umožňuje obejít kontrolu zabezpečení prostředků API pro požadavky IBM MQ přicházející z jednoho systému (například testovací systém, TESTCICS,), ale implementovat je pro jiný (například produkční systém, PRODCICS).

**Poznámka:** Pokud jste nastavili ID uživatele adresního prostoru produktu CICS s atributem "trusted" ve třídě STARTED nebo v tabulce spuštěných procedur RACF ICHRIN03, potlačí všechny kontroly ID uživatele adresního prostoru CICS vytvořeného profilem RESLEVEL pro vašeho správce front (to znamená, že správce front neprovádí kontrolu zabezpečení pro adresní prostor CICS ). Další informace naleznete v příručce *CICS Transaction Server for z/OS V3.2 RACF Security Guide*.

V následující tabulce jsou uvedeny kontroly provedené u připojení produktu CICS .

<i>Tabulka 50. Kontroly provedené na různých úrovních přístupu RACF pro připojení CICS</i>	
<b>RACF úroveň přístupu</b>	<b>Stupeň kontroly</b>
ŽÁDNÉ	Produkt IBM MQ zkontroluje ID uživatele adresního prostoru CICS a ID uživatele transakce.
READ (čtení)	IBM MQ kontroluje pouze ID uživatele adresního prostoru CICS .
AKTUALIZOVAT	Je-li transakce definována na CICS s parametrem RESSEC (YES), produkt IBM MQ zkontroluje ID uživatele adresního prostoru CICS a ID uživatele transakce.
AKTUALIZOVAT	Je-li transakce definována na CICS s RESESEC (NO), IBM MQ kontroluje pouze ID uživatele adresního prostoru CICS .
CONTROL nebo ALTER	Produkt IBM MQ nekontroluje žádná ID uživatelů.

### **Připojení RESLEVEL a IMS**

Je-li pro připojení produktu IMS provedena kontrola zabezpečení prostředků rozhraní API, je při výchozím nastavení zaškrtnuto dvě ID uživatelů. Pomocí nastavení profilu RESLEVEL můžete změnit, která ID uživatele se kontrolují.

Je-li pro připojení produktu IMS provedena kontrola zabezpečení prostředků rozhraní API, je při výchozím nastavení ověřeno, zda je přístup k prostředku povolen, jsou zkontrolována dvě ID uživatelů.



První zaškrtnuté ID uživatele je adresní prostor oblasti IMS . To je převzato buď z pole USER z zakázkového listu, nebo z ID uživatele přiřazeného oblasti ze třídy z/OS STARTED nebo z tabulky spuštěných procedur (SPT).

Druhé kontrolované ID uživatele je přidruženo k práci, která se provádí v závislé oblasti. Určí se podle typu závislé oblasti, jak ukazuje [Jak je určeno druhé ID uživatele pro připojení IMS](#).

Pokud buď první, nebo druhé ID uživatele produktu IMS nemá přístup k prostředku, požadavek selže s kódem dokončení MQRN\_NOT\_AUTHORIZED.

The setting of IBM MQ RESLEVEL profiles cannot alter the user ID under which IMS transactions are scheduled from the IBM-supplied MQ-IMS trigger monitor program CSQQTRMN. Toto ID uživatele je PSBNAME monitoru spouštěčů, což je standardně CSQQTRMN.

## Jak RESLEVEL může ovlivnit provedené kontroly

V závislosti na tom, jak nastavíte profil RESLEVEL, můžete změnit, která ID uživatelů se kontrolují při požadavku na přístup k prostředku. Možné kontroly jsou:

- Zkontrolujte ID uživatele adresního prostoru oblasti IMS a druhé ID uživatele nebo alternativní ID uživatele.
- Zkontrolujte pouze ID uživatele adresního prostoru oblasti IMS .
- Nekontrolovat žádná ID uživatelů.

V následující tabulce jsou uvedeny kontroly provedené u připojení produktu IMS .

<i>Tabulka 51. Kontroly provedené na různých úrovních přístupu RACF pro připojení IMS</i>	
<b>RACF úroveň přístupu</b>	<b>Stupeň kontroly</b>
ŽÁDNÉ	Zkontrolujte ID uživatele adresního prostoru IMS a ID uživatele druhého uživatele IMS nebo alternativní ID uživatele.
READ (čtení)	Zkontrolujte ID uživatele adresního prostoru IMS .
AKTUALIZOVAT	Zkontrolujte ID uživatele adresního prostoru IMS .
CONTROL	Žádná kontrola.
ALTER	Žádná kontrola.

## **RESLEVEL a připojení inicializátoru kanálu**

Je-li při kontrole zabezpečení pomocí rozhraní API kanálu provedena kontrola zabezpečení prostředku rozhraní API, jsou zaškrtnutá dvě ID uživatelů. Pomocí nastavení profilu RESLEVEL můžete změnit, která ID uživatele se kontrolují.

Je-li při kontrole zabezpečení pomocí rozhraní API kanálu provedena kontrola zabezpečení prostředku rozhraní API, kontrolují se standardně dvě ID uživatelů, aby bylo možné zjistit, zda je přístup k prostředku povolen.

Kontrolují se ID uživatele, která jsou uvedena atributem kanálu MCAUSER, který byl přijat ze sítě, z adresního prostoru inicializátoru kanálu nebo alternativního ID uživatele pro deskriptor zprávy. Která ID uživatelů jsou kontrolována, závisí na komunikačním protokolu, který používáte, a na nastavení atributu PUTAUT kanálu. Další informace viz [“ID uživatele použítá inicializátorem kanálu”](#) na stránce 225.

Pokud jedno z těchto ID uživatelů nemá přístup k prostředku, požadavek selže s kódem dokončení MQRN\_NOT\_AUTHORIZED.

## Jak RESLEVEL může ovlivnit provedené kontroly

V závislosti na tom, jak nastavíte profil RESLEVEL, můžete změnit, která ID uživatelů se kontrolují při požadavku na přístup k prostředku a kolik jich je zkontrolováno.

Následující tabulka zobrazuje kontroly provedené pro připojení inicializátoru kanálu a pro všechny kanály od té doby, co používají toto připojení.

<i>Tabulka 52. Kontroly provedené na různých úrovních přístupu RACF pro připojení inicializátoru kanálu</i>	
<b>RACF úroveň přístupu</b>	<b>Stupeň kontroly</b>
ŽÁDNÉ	Zkontrolujte dvě ID uživatelů.
READ (čtení)	Zkontrolujte jedno ID uživatele.
AKTUALIZOVAT	Zkontrolujte jedno ID uživatele.
CONTROL	Žádná kontrola.
ALTER	Žádná kontrola.

**Poznámka:** Definice kontrolovaných ID uživatelů viz [“ID uživatele použitá inicializátorem kanálu”](#) na stránce 225 .

### **RESLEVEL a řazení do front v rámci skupiny**

Je-li správcem front v rámci skupiny provedena kontrola zabezpečení prostředků rozhraní API, je při výchozím nastavení zkontrolováno, zda je přístup k prostředku povolen, a to pomocí dvou ID uživatelů. Pomocí nastavení profilu RESLEVEL můžete změnit, která ID uživatelů se budou kontrolovat.

Ověřovanou ID uživatelů může být ID uživatele určené atributem IGQUSER přijímajícího správce front, ID uživatele správce front v rámci skupiny sdílení front, který zprávu vložil do systému SYSTEM.QSG.TRANSMIT.QUEUE, nebo alternativní ID uživatele zadané v poli *UserIdentifier* deskriptoru zpráv zprávy. Další informace viz [“ID uživatelů použitá agentem front v rámci skupiny”](#) na stránce 229.

Vzhledem k tomu, že agent fronty v rámci skupiny je interní úloha správce front, nevydá explicitní žádost o připojení a pracuje pod ID uživatele správce front. Agent front intra-group se spustí při inicializaci správce front. Během inicializace agenta řazení do front v rámci skupiny produkt IBM MQ kontroluje přístup, který má ID uživatele přidružený ke správci front k profilu ve třídě MQADMIN s názvem:

```
hlq.RESLEVEL
```

Tato kontrola se provádí vždy, pokud nebyl nastaven přepínač hlq.NO.SUBSYS.SECURITY .

Pokud neexistuje žádný profil RESLEVEL, IBM MQ povolí kontrolu pro dvě ID uživatelů. Existuje-li profil RESLEVEL, úroveň kontroly závisí na úrovni přístupu uděleného ID uživatele správce front pro daný profil. Kontroly provedené při různých úrovních přístupu produktu RACF(r) pro správce front v rámci skupiny zobrazují kontroly provedené u agenta řazení do front v rámci skupiny.

<i>Tabulka 53. Kontroly provedené na různých úrovních přístupu produktu RACF pro agenta intra-group queuing Agent</i>	
<b>RACF úroveň přístupu</b>	<b>Stupeň kontroly</b>
ŽÁDNÉ	Zkontrolujte dvě ID uživatelů.
READ (čtení)	Zkontrolujte jedno ID uživatele.
AKTUALIZOVAT	Zkontrolujte jedno ID uživatele.
CONTROL	Žádná kontrola.
ALTER	Žádná kontrola.

**Poznámka:** Definice kontrolovaných ID uživatelů viz [“ID uživatelů použitá agentem front v rámci skupiny”](#) na stránce 229 .

Změní-li se oprávnění udělená profilu RESLEVEL pro ID uživatele správce front, musí být agent fronty v rámci skupiny zastaven a restartován, aby bylo možné nová oprávnění vybrat. Protože neexistuje žádný způsob, jak nezávisle zastavit a restartovat agenta intra-group queuing, musí být správce front zastaven a restartován, aby toho bylo možné dosáhnout.

### **RESLEVEL a ID uživatelů zkontrolováno**

Příklad nastavení profilu RESLEVEL a udělení přístupu k němu.

Kontrola ID uživatele vzhledem k názvu profilu pro dávkové připojení prostřednictvím volby ID uživatele zkontrolována proti názvu profilu pro LU 6.2 a kanály připojení serveru TCP/IP ukazují, jak RESLEVEL ovlivňuje, která ID uživatelů jsou kontrolována pro různé požadavky MQI.

Předpokládejme například, že máte správce front s názvem QM66 s následujícími požadavky:

- Uživatel WS21B má být vynechán ze zabezpečení prostředků.
- CICS spuštěná úloha WXNCICS běžící pod ID uživatele adresního prostoru CICSWXN má provést úplnou kontrolu prostředků pouze pro transakce definované s parametrem RESSEC (YES).

Chcete-li definovat příslušný profil RESLEVEL, zadejte následující příkaz RACF :

```
RDEFINE MQADMIN QM66.RESLEVEL UACC(NONE)
```

Poté udělte uživatelům přístup k tomuto profilu pomocí následujících příkazů:

```
PERMIT QM66.RESLEVEL CLASS(MQADMIN) ID(WS21B) ACCESS(CONTROL)
PERMIT QM66.RESLEVEL CLASS(MQADMIN) ID(CICSWXN) ACCESS(UPDATE)
```

Provedete-li tyto změny během připojení uživatelských jmen ke správci front QM66, uživatelé se musí před změnou připojení znovu odpojit a znovu připojit.

Není-li zabezpečení subsystému aktivní, když se uživatel připojuje, ale když je tento uživatel stále připojen, stane se zabezpečení podsystému aktivní, kontrola zabezpečení celého prostředku se použije na uživatele. Aby bylo možné získat správné zpracování RESLEVEL, musí se uživatel znovu připojit.

### **ID uživatele pro kontrolu zabezpečení**

Produkt IBM MQ spouští kontroly zabezpečení založené na ID uživatelů přidružených k uživatelům, terminálům, aplikacím a dalším prostředkům. Tato kolekce témat uvádí, která ID uživatelů se používají pro každý typ kontroly zabezpečení.

#### **ID uživatele pro zabezpečení připojení**

ID uživatele použité pro zabezpečení připojení závisí na typu připojení.

Typ připojení	Obsah ID uživatele
Dávkové připojení	ID uživatele připojované úlohy. Příklad: <ul style="list-style-type: none"> <li>• ID uživatele TSO</li> <li>• ID uživatele přiřazené dávkové úloze pomocí parametru USER JCL</li> <li>• ID uživatele přiřazeného ke spuštěné úloze podle třídy STARTED nebo tabulky spuštěných procedur</li> </ul>
CICS připojení	ID uživatele adresního prostoru CICS .
IMS připojení	ID uživatele adresního prostoru oblasti IMS .
Připojení inicializátoru kanálu	ID uživatele adresního prostoru iniciátoru kanálu.

### **ID uživatele pro zabezpečení příkazů a zabezpečení prostředků příkazů**

ID uživatele použité pro zabezpečení příkazů nebo zabezpečení prostředků příkazů závisí na tom, odkud je příkaz vydán.

<b>Vydáno z ...</b>	<b>Obsah ID uživatele</b>
CSQINP1, CSQINP2, nebo CSQINPT	Neprovede se žádná kontrola.
Vstupní fronta systémového příkazu	ID uživatele nalezeného v <i>UserIdentifier</i> deskriptoru zprávy, který obsahuje příkaz. Pokud zpráva neobsahuje <i>UserIdentifier</i> , předá se správci zabezpečení ID uživatele mezery.
Konzola	ID uživatele přihlášené na konzolu. Není-li konzola přihlášená, výchozí ID uživatele nastavené systémovým parametrem CMDUSER v souboru CSQ6SYSP.  Chcete-li vydávat příkazy z konzoly, musí mít konzola atribut z/OS SYS AUTHORITY.
Konzola SDSF/TSO	TSO nebo ID uživatele úlohy.
Ovládací panely a ovládací panely	ID uživatele TSO.  Chcete-li používat operace a ovládací panely, musíte mít příslušné oprávnění k vydávání příkazů odpovídajících vámi vybízným akcím. Kromě toho musíte mít přístup pro čtení ke všem položkám hlq.DISPLAY. Profily <i>objektu</i> ve třídě MQCMD5, protože panely používají různé příkazy DISPLAY ke shromažďování informací, které mají k dispozici.
MGCRE	Je-li MGCRE použito s UTOKEN, ID uživatele v UTOKEN.  Je-li MGCRE vydán bez použití UTOKEN, použije se TSO nebo ID uživatele úlohy.
CSQOUTIL	ID uživatele úlohy.
KALKUNIT	ID uživatele úlohy.
CSQINPX	ID uživatele adresního prostoru inicializátoru kanálu.

### **ID uživatelů pro zabezpečení prostředků (MQOPEN, MQSUB a MQPUT1)**

Tyto informace zobrazují obsah ID uživatelů pro běžné a alternativní ID uživatele pro každý typ připojení. Počet kontrol je definován profilem RESLEVEL. ID uživatele, které bylo zkontrolováno, je použito pro volání **MQOPEN, MQSUB** nebo **MQPUT1**.

**Poznámka:** Všechna pole ID uživatele se kontrolují přesně tak, jak jsou přijata. Nejsou provedeny žádné konverze, a například tři pole s ID uživatele obsahující "Bob", "BOB" a "bob" nejsou ekvivalentní.

*ID uživatele byla zkontrolována pro připojení dávky*

ID uživatele kontrolované pro dávkové připojení závisí na tom, jak je úloha spuštěna a zda bylo zadáno alternativní ID uživatele.

<i>Tabulka 54. Kontrola ID uživatele vzhledem k názvu profilu pro dávkové připojení</i>			
<b>Alternativní ID uživatele zadané při otevření?</b>	<b>hlq.ALTERNATE.USER.userid</b>	<b>Profil hlq.CONTEXT.queueName</b>	<b>Profil hlq.resourcename</b>
<b>Ne</b>	-	Úloha	Úloha
<b>Ano</b>	Úloha	Úloha	KLÁVESA ALT

Klíč:

## KLÁVESA ALT

Alternativní ID uživatele.

### Úloha

- ID uživatele pro přihlášení TSO nebo USS.
- ID uživatele přiřazené dávkové úloze.
- ID uživatele přiřazeného ke spuštění úloze podle třídy STARTED nebo tabulky spuštěných procedur.
- ID uživatele přidružené k provádění uložené procedury Db2

Dávková úloha provádí příkaz MQPUT1 do fronty s názvem Q1 s volbou RESLEVEL nastaveným na hodnotu READ a alternativní kontrola ID uživatele vypnuta.

Kontroly provedené na různých úrovních přístupu RACF(r) pro dávkové připojení a Kontrola ID uživatele vzhledem k názvu profilu pro dávkové připojení ukazují, že ID uživatele úlohy je zkontrolováno proti profilu hlq.Q1.

*ID uživatelů zkontrolována pro připojení CICS*

ID uživatelů kontrolována pro připojení CICS závisí na tom, zda má být provedena jedna nebo dvě kontroly a zda je zadáno alternativní ID uživatele.

Alternativní ID uživatele zadané při otevření?	hlq.ALTERNATE.USER.userid	Profil hlq.CONTEXT.queueaname	Profil hlq.resourcename
<b>Ne, 1 kontrola</b>	-	PÍ	PÍ
<b>Ne, 2 kontroly</b>	-	ADS + TXN	ADS + TXN
<b>Ano, 1 kontrola</b>	PÍ	PÍ	PÍ
<b>Ano, 2 kontroly</b>	ADS + TXN	ADS + TXN	ADS + ALT

Klíč:

## KLÁVESA ALT

Jméno alternativního uživatele

### PÍ

ID uživatele přidružené k dávkové úloze CICS nebo, pokud je CICS spuštěn jako spuštěná úloha, přes třídu STARTED nebo tabulku spuštěných procedur.

### TXN

ID uživatele přidružené k transakci CICS . Toto je obvykle ID uživatele terminálu, který spustil transakci. Může to být CICS DFLTUSER, Terminál zabezpečení PRESET nebo ručně přihlášený uživatel.

Určete ID uživatele, která se kontrolují za následujících podmínek:

- Úroveň přístupu RACF k profilu RESLEVEL, pro ID uživatele adresního prostoru CICS je nastavena na hodnotu NONE.
- Volání MQOPEN je vytvořeno proti frontě s MQOO\_OUTPUT a MQOO\_PASS\_IDENTITY\_CONTEXT.

Nejprve si prohlédněte, kolik ID uživatelů produktu CICS je kontrolováno na základě ID uživatele CICS adresního prostoru uživatele k přístupu k profilu RESLEVEL. V produktu Tabulka 50 na stránce 219 v tématu “Připojení RESLEVEL a CICS” na stránce 219 jsou zkontrolována dvě ID uživatelů, je-li profil RESLEVEL nastaven na hodnotu NONE. Pak od Tabulka 55 na stránce 224 jsou tyto kontroly prováděny:

- Příkaz hlq.ALTERNATE.USER.userid není kontrolován.
- Profil hlq.CONTEXT.queueaname je kontrolován s ID uživatele adresního prostoru CICS i ID uživatele transakce CICS .
- Profil hlq.resourcename je zkontrolován jak s ID uživatele adresního prostoru CICS , tak i s ID uživatele transakce CICS .

To znamená, že jsou provedeny čtyři kontroly zabezpečení pro toto volání MQOPEN .

*ID uživatelů zkontrolována pro připojení IMS*

ID uživatelů kontrolována pro připojení produktu IMS závisí na tom, zda má být provedena jedna nebo dvě kontroly a zda je určeno alternativní ID uživatele. Je-li zaškrtnuté druhé ID uživatele, závisí na typu závislé oblasti a na tom, která ID uživatele jsou k dispozici.

*Tabulka 56. Kontrola ID uživatele pro jméno profilu pro IMS-type ID uživatele*

<b>Alternativní ID uživatele zadané při otevření?</b>	<b>hlq.ALTERNATE.USER.userid</b>	<b>Profil hlq.CONTEXT.queuename</b>	<b>Profil hlq.resourcename</b>
<b>Ne, 1 kontrola</b>	-	REG.	REG.
<b>Ne, 2 kontroly</b>	-	REG + SEC	REG + SEC
<b>Ano, 1 kontrola</b>	REG.	REG.	REG.
<b>Ano, 2 kontroly</b>	REG + SEC	REG + SEC	REG. NEBO

Klíč:

**KLÁVESA ALT**

Alternativní ID uživatele.

**REG.**

ID uživatele je obvykle nastaveno prostřednictvím třídy STARTED nebo v tabulce spuštěných procedur nebo, pokud je IMS spuštěný, z odeslané úlohy parametrem USER JCL.

**Sek**

Druhé ID uživatele je přidruženo k práci, která se provádí v závislé oblasti. Je určen podle [Tabulka 57](#) na stránce 225.

*Tabulka 57. Jak je určeno druhé ID uživatele pro připojení produktu IMS*

<b>Typy závislých oblastí</b>	<b>Hierarchie pro určení druhého ID uživatele</b>
<ul style="list-style-type: none"> <li>• Byla vydána zpráva BMP a bylo vydáno úspěšné GET UNIQUE.</li> <li>• IFP a GET UNIQUE vydané.</li> <li>• MPP.</li> </ul>	<p>ID uživatele přidružené k transakci IMS , pokud je uživatel přihlášen.</p> <p>Název LTERM, pokud je dostupný.</p> <p>PSBNAME.</p>
<ul style="list-style-type: none"> <li>• Zpráva BMP vyvolaná a úspěšná metoda GET UNIQUE nebyla vydána.</li> <li>• BMP neřízená zprávou.</li> <li>• IFP a GET UNIQUE nebyly vydány.</li> </ul>	<p>ID uživatele přidružené k adresnímu prostoru oblasti závislé na IMS , pokud se nejedná o všechny mezery nebo samé nuly.</p> <p>PSBNAME.</p>

*ID uživatele použitá iniciálátorem kanálu*

Tato kolekce témat popisuje používaná a zaškrtnutá jména uživatelů pro přijímací kanály a pro klientské požadavky MQI vydané přes kanály připojení serveru. Informace jsou poskytnuty pro TCP/IP a pro LU6.2

K určení typu použité kontroly zabezpečení můžete použít parametr PUTAUT v definici přijímajícího kanálu. Chcete-li zajistit konzistentní kontrolu zabezpečení v rámci celé sítě produktu IBM MQ , můžete použít volby ONLYMCA a ALTMCA.

K určení identifikátoru uživatele použitého agentem MCA můžete použít příkaz DISPLAY CHSTATUS.

*Příjem kanálů pomocí protokolu TCP/IP*

Kontrolována ID uživatelů závisí na volbě PUTAUT kanálu a na tom, zda má být provedena jedna nebo dvě kontroly.

Tabulka 58. ID uživatelů byly zkontrolována proti názvu profilu pro kanály TCP/IP			
Volba PUTAUT zadaná v kanálu příjemce nebo žadatele	hlq.ALTERNATE.USER.userid	Profil hlq.CONTEXT.queueName	Profil hlq.resourcename
<b>DEF, 1 kontrola</b>	-	CHL	CHL
<b>DEF, 2 kontroly</b>	-	CHL + MCA	CHL + MCA
<b>Kontrola CTX, 1</b>	CHL	CHL	CHL
<b>CTX, 2 kontroly</b>	CHL + MCA	CHL + MCA	CHL + ALT
<b>ONLYMCA, 1 kontrola</b>	-	MCA	MCA
<b>ONLYMCA, 2 kontroly</b>	-	MCA	MCA
<b>ALTMCA, 1 kontrola</b>	MCA	MCA	MCA
<b>ALTMCA, 2 kontroly</b>	MCA	MCA	MCA + ALT

Klíč:

#### **MCA (ID uživatele MCA)**

ID uživatele zadané pro atribut kanálu MCAUSER na přijímači; je-li prázdné, použije se ID uživatele adresního prostoru kanálu příjemce na straně příjemce nebo žadatele.

#### **CHL (ID uživatele kanálu)**

V TCP/IP není zabezpečení podporováno komunikačním systémem pro kanál. Je-li použito zabezpečení SSL (Secure Sockets Layer) a byl od partnera přenášen digitální certifikát, použije se ID uživatele přidružené k tomuto certifikátu (je-li nainstalován) nebo ID uživatele přidružené k odpovídajícímu filtru, který byl nalezen pomocí filtrování certifikátů (CNF) produktu RACF. Pokud není nalezeno žádné přidružené ID uživatele nebo pokud se nepoužívá SSL, použije se ID uživatele adresního prostoru iniciátoru kanálu přijímajícího nebo žadatelského konce jako ID uživatele kanálu na kanálech definovaných s parametrem PUTAUT nastaveným na DEF nebo CTX.

**Poznámka:** Použití filtrování názvu certifikátu produktu RACF (CNF) vám umožňuje přiřadit stejné ID uživatele produktu RACF k více vzdáleným uživatelům, například všechny uživatele ve stejné organizační jednotce, kteří by přirozeně měli mít stejné oprávnění zabezpečení. To znamená, že server nemusí mít kopii certifikátu všech možných vzdálených koncových uživatelů po celém světě a výrazně zjednodušuje správu a distribuci certifikátů.

Je-li parametr PUTAUT nastaven na hodnotu ONLYMCA nebo ALTMCA pro daný kanál, je ID uživatele kanálu ignorováno a použije se ID uživatele MCA přijímače nebo žadatele. To platí také pro kanály TCP/IP používající zabezpečení SSL.

#### **ALT (Alternativní ID uživatele)**

ID uživatele z informací o kontextu (to znamená pole *UserIdentifier*) v rámci deskriptoru zprávy. Toto ID uživatele je přesunuto do pole *AlternateUserID* v deskriptoru objektu před zadáním volání **MQOPEN** nebo **MQPUT1** pro cílovou frontou.

#### *Přijem kanálů pomocí LU 6.2*

Kontrolovaná ID uživatelů závisí na volbě PUTAUT kanálu a na tom, zda má být provedena jedna nebo dvě kontroly.

Tabulka 59. ID uživatelů zkontrolována oproti názvu profilu pro kanály LU 6.2

Volba PUTAUT zadaná v kanálu příjemce nebo žadatele	hlq.ALTERNATE.USER.userid	Profil hlq.CONTEXT.queue name	Profil hlq.resourcename
<b>DEF, 1 kontrola</b>	-	CHL	CHL
<b>DEF, 2 kontroly</b>	-	CHL + MCA	CHL + MCA
<b>Kontrola CTX, 1</b>	CHL	CHL	CHL
<b>CTX, 2 kontroly</b>	CHL + MCA	CHL + MCA	CHL + ALT
<b>ONLYMCA, 1 kontrola</b>	-	MCA	MCA
<b>ONLYMCA, 2 kontroly</b>	-	MCA	MCA
<b>ALTMCA, 1 kontrola</b>	MCA	MCA	MCA
<b>ALTMCA, 2 kontroly</b>	MCA	MCA	MCA + ALT

Klíč:

#### **MCA (ID uživatele MCA)**

ID uživatele zadané pro atribut kanálu MCAUSER na přijímači; je-li prázdné, použije se ID uživatele adresního prostoru kanálu příjemce na straně příjemce nebo žadatele.

#### **CHL (ID uživatele kanálu)**

##### **Kanály žadatele-server**

Pokud je kanál spuštěn od žadatele, neexistuje žádná příležitost pro přijetí ID uživatele sítě (ID uživatele kanálu).

Je-li parametr PUTAUT nastaven na DEF nebo CTX na žadatelský kanál, ID uživatele kanálu je ID adresního prostoru iniciátoru kanálu žadatele, protože není přijato žádné ID uživatele ze sítě.

Je-li parametr PUTAUT nastaven na hodnotu ONLYMCA nebo ALTMCA, ID uživatele kanálu se ignoruje a použije se ID uživatele MCA pro žadatele.

##### **Další typy kanálů**

Je-li parametr PUTAUT nastaven na DEF nebo CTX na přijímači nebo žadatelský kanál, ID uživatele kanálu je ID uživatele přijaté z komunikačního systému, když je kanál iniciován.

- Pokud je odesílací kanál v systému z/OS, přijaté ID uživatele kanálu je ID uživatele adresního prostoru kanálu iniciátoru kanálu odesílatele.
- Je-li odesílající kanál na jiné platformě (například AIX nebo HP-UX), přijaté ID uživatele kanálu je obvykle poskytováno parametrem USERID definice kanálu.

Pokud je přijaté ID uživatele prázdné, nebo pokud není přijato žádné ID uživatele, použije se ID uživatele kanálu.

#### **ALT (Alternativní ID uživatele)**

ID uživatele z informací o kontextu (to znamená pole *UserIdentifier*) v rámci deskriptoru zprávy. Toto ID uživatele je přesunuto do pole *AlternateUserID* v deskriptoru objektu před voláním příkazu MQOPEN nebo MQPUT1 pro cílovou frontou.

##### *Požadavky klienta MQI*

Lze použít různá ID uživatelů, v závislosti na tom, které ID uživatele a proměnné prostředí byly nastaveny. Tato ID uživatelů jsou zkontrolována proti různým profilům, v závislosti na použité volbě PUTAUT a na tom, zda je zadáno alternativní ID uživatele.



Tato sekce popisuje ID uživatelů, která byla zkontrolována pro požadavky klienta MQI vydané prostřednictvím kanálů připojení serveru pro protokol TCP/IP a LU 6.2. ID uživatele MCA a ID uživatele kanálu jsou určeny pro kanály TCP/IP a LU 6.2 popsané v předchozích sekcích.

Pro kanály připojení serveru se použije ID uživatele přijaté od klienta, je-li atribut MCAUSER prázdný.

Další informace viz [“Řízení přístupu pro klienty”](#) na stránce 83.

Pro požadavky klienta **MQOPEN**, **MQSUBa** **MQPUT1** použijte následující pravidla k určení profilu, který se kontroluje:

- Pokud je v požadavku uvedeno oprávnění alternativního uživatele, provede se kontrola proti příkazu *hlq.ALTERNATE.USER*. Profil *userid*.
- Pokud požadavek specifikuje oprávnění ke kontextu, provede se kontrola proti *hlq.KONTEXT*. Profil *queueName*.
- Pro všechny požadavky **MQOPEN**, **MQSUBa** **MQPUT1** se provádí kontrola na profilu *hlq.resourcename*.

Když jste určili, které profily se kontrolují, použijte následující tabulku k určení, která ID uživatelů jsou kontrolována proti těmto profilům.

*Tabulka 60. ID uživatelů byly zkontrolovány proti názvu profilu pro LU 6.2 a kanály připojení k serveru TCP/IP*

<b>Volba PUTAUT zadaná v kanálu připojení serveru</b>	<b>Alternativní ID uživatele zadané při otevření?</b>	<b>hlq.ALTERNATE.USER.userid</b>	<b>Profil hlq.CONTEXT.queueName</b>	<b>Profil hlq.resourcename</b>
<b>DEF, 1 kontrola</b>	Ne	-	CHL	CHL
<b>DEF, 1 kontrola</b>	Ano	CHL	CHL	CHL
<b>DEF, 2 kontroly</b>	Ne	-	CHL + MCA	CHL + MCA
<b>DEF, 2 kontroly</b>	Ano	CHL + MCA	CHL + MCA	CHL + ALT
<b>ONLYMCA, 1 kontrola</b>	Ne	-	MCA	MCA
<b>ONLYMCA, 1 kontrola</b>	Ano	MCA	MCA	MCA
<b>ONLYMCA, 2 kontroly</b>	Ne	-	MCA	MCA
<b>ONLYMCA, 2 kontroly</b>	Ano	MCA	MCA	MCA + ALT

Klíč:

**MCA (ID uživatele MCA)**

ID uživatele zadané pro atribut kanálu MCAUSER na serveru-connection; je-li prázdné, použije se ID uživatele adresního prostoru kanálu kanálu.

**CHL (ID uživatele kanálu)**

V TCP/IP není zabezpečení podporováno komunikačním systémem pro kanál. Je-li použito zabezpečení SSL (Secure Sockets Layer) a byl od partnera přenášen digitální certifikát, použije se ID uživatele přidružené k tomuto certifikátu (je-li nainstalován) nebo ID uživatele přidružené k odpovídajícímu filtru, který byl nalezen pomocí filtrování certifikátů (CNF) produktu RACF. Pokud

není nalezeno žádné přidružené ID uživatele nebo pokud není použito zabezpečení SSL, použije se ID uživatele adresního prostoru iniciátoru kanálu jako ID uživatele kanálu v kanálech definovaných s parametrem PUTAUT nastaveným na DEF nebo CTX.

**Poznámka:** Použití filtrování názvu certifikátu produktu RACF (CNF) vám umožňuje přiřadit stejné ID uživatele produktu RACF k více vzdáleným uživatelům, například všechny uživatele ve stejné organizační jednotce, kteří by přirozeně měli mít stejné oprávnění zabezpečení. To znamená, že server nemusí mít kopii certifikátu všech možných vzdálených koncových uživatelů po celém světě a výrazně zjednodušuje správu a distribuci certifikátů.

Je-li parametr PUTAUT nastaven na hodnotu ONLYMCA nebo ALTMCA pro daný kanál, je ID uživatele kanálu ignorováno a použije se ID uživatele MCA kanálu připojení serveru. To platí také pro kanály TCP/IP používající zabezpečení SSL.

### ALT (Alternativní ID uživatele)

ID uživatele z informací o kontextu (to znamená pole *UserIdentifier*) v rámci deskriptoru zprávy. Toto ID uživatele se přesune do pole *AlternateUserID* v objektu nebo deskriptoru odběru, dříve než je vydán příkaz **MQOPEN**, **MQSUB** nebo **MQPUT1** jménem klientské aplikace.

#### *Příklad inicializátoru kanálu*

Příklad toho, jak jsou ID uživatelů kontrolována proti profilům RACF .

Uživatel provede operaci **MQPUT1** pro frontu ve správci front QM01 , která se přeloží do fronty s názvem QB ve správci front QM02. Zpráva se odešle na kanál TCP/IP s názvem QM01.TO.QM02. Hodnota RESLEVEL je nastavena na hodnotu NONE a operace otevření se provádí s alternativním ID uživatele a kontrolou kontextu. Definice přijímacího kanálu má hodnotu PUTAUT (CTX) a ID uživatele MCA je nastaveno. Která ID uživatele se používají v přijímajícím kanálu k vložení zprávy do fronty QB?

**Odpověď:** [Tabulka 52 na stránce 221](#) zobrazuje, že jsou zkontrolována dvě ID uživatelů, protože RESLEVEL je nastaven na NONE.

[Tabulka 58 na stránce 226](#) ukazuje, že s parametrem PUTAUT nastaveným na CTX a 2, jsou zkontrolována následující ID uživatelů:

- ID uživatele iniciátoru kanálu a ID uživatele MCAUSER se kontrolují proti příkazu hlq.ALTERNATE.USER.userid .
- ID uživatele iniciátoru kanálu a ID uživatele MCAUSER se kontrolují proti profilu hlq.CONTEXT.queueename .
- ID uživatele iniciátoru kanálu a alternativní ID uživatele uvedené v deskriptoru zpráv (MQMD) se kontrolují proti profilu hlq.Q2 .

#### *ID uživatelů použitá agentem front v rámci skupiny*

ID uživatelů, která jsou zkontrolována při otevření cílových front pro správce front v rámci skupiny, jsou určovány hodnotami atributů správce front IGQAUT a IGQUSER.

Možné ID uživatele jsou:

### **ID uživatele pro řazení do front v rámci skupiny (IGQ)**

ID uživatele určené atributem IGQUSER přijímacího správce front. Je-li tato hodnota nastavena na prázdné místo, použije se ID uživatele přijímacího správce front. Vzhledem k tomu, že přijímací správce front má oprávnění pro přístup ke všem definovaným frontám, kontroly zabezpečení se u ID uživatele přijímacího správce front neprovádějí. V tomto případě:

- Pokud má být zkontrolováno pouze jedno ID uživatele a ID uživatele přijímacího správce front, žádné kontroly zabezpečení se neprovedou. To může nastat, když je IGQAUT nastaveno na ONLYIGQ nebo ALTIGQ.
- Pokud mají být zkontrolována dvě ID uživatelů a jedno z ID uživatelů je ID přijímacího správce front, kontroly zabezpečení se provedou pouze pro jiné ID uživatele. To může nastat, když je IGQAUT nastaveno na DEF, CTX nebo ALTIGQ.
- Pokud mají být zkontrolována dvě ID uživatelů a jsou-li jména uživatelů přijímacím správcem front, žádné kontroly zabezpečení se neprovedou. To může nastat, když je IGQAUT nastaveno na ONLYIGQ.

### Odeslání ID uživatele správce front (SND)

ID uživatele správce front v rámci skupiny sdílení front, který vložil zprávu do systému SYSTEM.QSG.TRANSMIT.QUEUE.

### Alternativní ID uživatele (ALT)

ID uživatele uvedené v poli *UserIdentifier* v deskriptoru zprávy zprávy.

Tabulka 61. ID uživatelů zkontrolovaná vzhledem k názvu profilu pro řazení do front v rámci skupiny			
Volba IGQAUT zadaná v přijímajícím správci front	hlq.ALTERNATE.USER.userid	Profil hlq.CONTEXT.queue name	Profil hlq.resourcename
<b>DEF, 1 kontrola</b>	-	SND	SND
<b>DEF, 2 kontroly</b>	-	SND + IGQ	SND + IGQ
<b>Kontrola CTX, 1</b>	SND	SND	SND
<b>CTX, 2 kontroly</b>	SND + IGQ	SND + IGQ	SND + ALT
<b>ONLYIGQ, 1 kontrola</b>	-	IGQ	IGQ
<b>ONLYIGQ, 2 kontroly</b>	-	IGQ	IGQ
<b>ALTIGQ, 1 kontrola</b>	-	IGQ	IGQ
<b>ALTIGQ, 2 kontroly</b>	IGQ	IGQ	IGQ + ALT

Klíč:

#### KLÁVESA ALT

Alternativní ID uživatele.

#### IGQ

ID uživatele IGQ.

#### SND

Odesílá se ID uživatele správce front.

### Prázdné ID uživatele a úrovně UACC

Pokud dojde k mezerové ID uživatele, je přihlášen RACF nedefinovaný uživatel. Nepřidělte přístup k nedefinovanému uživateli v rozsahu bez omezení.

Prázdné ID uživatele může existovat, když uživatel manipuluje se zprávami pomocí kontextu nebo alternativního zabezpečení uživatele, nebo když IBM MQ projde prázdné ID uživatele. Prázdné ID uživatele se například použije, když je zpráva zapsána do vstupní fronty příkazového systému bez kontextu.

**Poznámka:** ID uživatele " \* " (To znamená, že znak hvězdička následovaný sedmi mezerami) je považován za nedefinované ID uživatele.

Příkaz IBM MQ předá prázdné ID uživatele do produktu RACF a je přihlášen RACF nedefinovaný uživatel. Všechny bezpečnostní kontroly pak použijí univerzální přístup (UACC) pro příslušný profil. V závislosti na tom, jak jste nastavili úroveň přístupu, UACC může dát nedefinovanému uživateli přístup s rozsahem platnosti.

Pokud například vydáte tento příkaz RACF z TSO:

```
RDEFINE MQQUEUE Q.AVAILABLE.TO.EVERYONE UACC(UPDATE)
```

Definujete profil, který povoluje uživatelem definované ID uživatelů z/OS (které nebyly vloženy do přístupového seznamu) a RACF nedefinované ID uživatele pro vkládání zpráv a získání zpráv od této fronty.

Chcete-li chránit před prázdnými ID uživatelů, musíte pečlivě plánovat úroveň přístupu a omezit počet osob, které mohou používat kontext a zabezpečení alternativního uživatele. Musíte zabránit osobám, které používají nedefinované ID uživatele produktu RACF, přístup k prostředkům, k jejichž přístupu nemají přístup. Zároveň však musíte povolit přístup osobám s definovanými uživatelskými ID. Chcete-li to provést, můžete zadat ID uživatele hvězdička (\*) v příkazu RACF PERMIT, který umožňuje přístup k prostředkům pro všechna definovaná ID uživatelů. Proto jsou všechna nedefinovaná ID uživatele (jako např. " \* ") jsou odepřený přístup. Například tyto příkazy RACF zabraňují RACF nedefinovanému ID uživatele získat přístup do fronty k vložení nebo získání zpráv:

```
RDEFINE MQQUEUE Q.AVAILABLE.TO.RACF.DEFINED.USERS.ONLY UACC(NONE)
PERMIT Q.AVAILABLE.TO.RACF.DEFINED.USERS.ONLY CLASS(MQQUEUE) ACCESS(UPDATE) ID(*)
```

## z/OS ID uživatelů a vícefaktorové ověření (MFA)

IBM Vícefaktorové ověření pro produkt z/OS umožňuje administrátorům zabezpečení produktu z/OS zlepšit ověřování SAF, a to tím, že požadování identifikovaných uživatelů používá více faktorů ověření (například jak heslo, tak šifrovací token) k přihlášení do systému z/OS. IBM MFA také poskytuje podporu pro jednorázové technologie generování jednorázového hesla, jako je např. RSA SecureId.

Pro většinu částí produkt IBM MQ neví o tom, jak uživatelé mají "přihlášení" k CICS nebo dávkovým systémům, které řídí IBM MQ práce, podepsaná na pověření ID uživatele je přidružena k úloze nebo adresnímu prostoru z/OS, a IBM MQ ji používá pro kontrolu autorizace k prostředkům. ID uživatele povolená pro MFA lze použít pro autorizaci k prostředkům produktu IBM MQ a k ověření pomocí tiketů použitých s mosty CICS a IMS.

**Důležité:** Při použití aplikací, jako je MQ Explorer, které předává ID uživatele a heslo pověření ve volání rozhraní MQCONN API s volbou *MQCSP\_AUTH\_USER\_ID\_AND\_PWD*, je však třeba použít speciální pokyny. IBM MQ nemá žádné zařízení, které by mělo předat další pověření na tento požadavek rozhraní API.

Omezení a případná náhradní řešení jsou popsána v následujícím textu.

### MQ Explorer

Produkt MQ Explorer nelze použít pro přihlášení k systému z/OS s ID uživatele, pro které je povoleno MFA povoleno, protože neexistuje žádné zařízení pro předání druhého ověřovacího faktoru z MQ Explorer na z/OS.

Kromě toho existují dva různé mechanismy, které používá MQ Explorer k opětnému použití ID uživatele a pověření hesla, které vyžaduje zvláštní pozornost, když se používají hesla v jednom okamžiku:

1. Produkt MQ Explorer má schopnost ukládat hesla v zamčeném formátu na lokálním počítači pro přihlášení později. Tato schopnost musí být zakázána, když se zobrazí výzva k zadání hesla při každém připojení ke správci front z/OS.

Chcete-li to provést, postupujte takto:

- a. Vyberte položku **Správci front**.
- b. V zobrazeném seznamu vyberte správce front, kterého vyžadujete, a pravým tlačítkem myši klepněte na příslušného správce front.
- c. Ze seznamu nabídky, který se zobrazí, vyberte volbu **Podrobnosti připojení**.
- d. Vyberte **Vlastnosti** z následujícího seznamu nabídky a zvolte kartu **ID uživatele**.

Ujistěte se, že jste vybrali přepínač **Výzva k zadání hesla**.

2. Různé operace v produktu MQ Explorer, jako je procházení zpráv ve frontách, testování odběrů atd., spouští nový podproces, který se autentizuje v produktu IBM MQ pomocí pověření, které bylo použito při přihlášení jako první. Vzhledem k tomu, že pověření hesla nelze znovu použít, nemůžete tyto operace použít.

Na úrovni konfigurace MFA jsou dvě možné náhradní řešení pro tyto problémy:

- Použijte vyloučení MFA pro ID aplikace, chcete-li vyloučit úlohy IBM MQ ze zpracování MFA dohromady. Chcete-li to provést, zadejte následující příkazy:

```
1. RDEFINE MFADEF MFABYPASS.USERID.<chinuser>
```

kde <chinuser> je ID uživatele na úrovni adresy iniciátoru kanálu (přidružené k inicializátoru kanálu prostřednictvím třídy STC).

```
2. PERMIT MFABYPASS.USERID.<chinuser> ACCESS(READ) ID(<explorer user>)
```

Další informace o tomto přístupu najdete v tématu [Vynechání aplikace IBM MFA pro aplikace](#).

- Použijte podporu typu out-of-band na MFA, která byla zavedena s IBM MFA 1.2. S tímto přístupem se předpřihlašujete k webovému serveru IBM MFA a navíc k vašemu ID uživatele a heslu zadejte další ověření, které je určeno prostřednictvím zásady. Server IBM MFA generuje pověření tokenu mezipaměti, které pak zadáte v dialogovém okně ověření produktu MQ Explorer . Administrátor zabezpečení může povolit, aby bylo toto pověření přehráno pro přiměřenou dobu, takže umožňuje normální použití MQ Explorer .

Další informace o tomto přístupu viz [Úvod do IBM MFA](#).

## Správa zabezpečení produktu IBM MQ for z/OS

Produkt IBM MQ používá tabulku v paměti k ukládání informací týkajících se jednotlivých uživatelů a žádostí o přístup jednotlivých uživatelů. Chcete-li efektivně spravovat tuto tabulku a snížit počet požadavků z produktu IBM MQ na externího správce zabezpečení (ESM), je k dispozici řada ovládacích prvků.

Tyto ovládací prvky jsou dostupné prostřednictvím jak operací, tak řídicích panelů a příkazů IBM MQ .

### Převěrování ID uživatele

Pokud byla například změněna definice RACF uživatele, který používá prostředky IBM MQ , například připojením uživatele k nové skupině, můžete správci front sdělit, aby tento uživatel znovu podepsal při příštím pokusu o přístup k prostředku IBM MQ . To můžete provést pomocí příkazu IBM MQ RVERIFY SECURITY.

- Uživatel HX0804 získává a umísťuje zprávy do front PAYROLL ve správci front PRD1. Avšak HX0804 nyní vyžaduje přístup k některým frontám PENSION ve stejném správci front (PRD1).
- Administrátor zabezpečení dat připojí uživatele HX0804 do skupiny RACF , která umožňuje přístup k frontám PENSION.
- Takže HX0804 má přístup k frontám PENSION okamžitě-tj. bez ukončení správce front PRD1nebo čeká na vypršení časového limitu HX0804 -musíte použít příkaz IBM MQ :

```
RVERIFY SECURITY(HX0804)
```

**Poznámka:** Pokud vypnete časový limit ID uživatele po dlouhou dobu (dny nebo týdny), zatímco je správce front spuštěn, musíte si zapamatovat spuštění příkazu RVERIFY SECURITY pro všechny uživatele, kteří byli odvolaní nebo odstraněni v této době.

### Časové limity ID uživatele

Po určité době nečinnosti můžete produkt IBM MQ odhlásit od správce front.

Když uživatel přistupuje k prostředku produktu IBM MQ , pokusí se správce front o přihlášení tohoto uživatele do správce front (je-li aktivní zabezpečení subsystému). To znamená, že je uživatel ověřen pro ESM. Tento uživatel zůstane přihlášen k produktu IBM MQ , dokud nebude správce front vypnut, nebo dokud ID uživatele *vypršelo* (ověření se neukončí) nebo se znovu ověří (reověřená).

Když dojde k vypršení časového limitu uživatele, je ID uživatele *odhlášen* ve správci front a všechny informace související s bezpečností uchované pro tohoto uživatele byly zrušeny. Odpisování a odhlášení uživatele v rámci správce front není zjevné pro aplikační program nebo pro uživatele.

Uživatelé jsou způsobilí pro vypršení časového limitu, když nepoužili žádné prostředky IBM MQ pro předem určenou dobu. Toto časové období je nastaveno pomocí příkazu MQSC ALTER SECURITY.

V příkazu ALTER SECURITY lze zadat dvě hodnoty:

### **VYPRŠENÍ ČASOVÉHO LIMITU**

Časové období v minutách, kdy nepoužívané ID uživatele a jeho přidružené prostředky mohou zůstat ve správci front IBM MQ .

### **INTERVAL**

Časové období v minutách mezi kontrolami ID uživatelů a jejich přidružených prostředků, aby bylo možné určit, zda vypršela platnost *TIMEOUT* .

Například, je-li hodnota *TIMEOUT* 30 a hodnota *INTERVAL* je 10, každé 10 minut IBM MQ kontroluje ID uživatelů a jejich přidružené prostředky, aby určil, zda nebyly některé z nich použity po dobu 30 minut. Pokud je nalezeno ID uživatele, jehož časový limit vypršel, je toto ID uživatele odhlášeno v rámci správce front. Dojde-li k nalezení všech informací o vypršení časového limitu přidružených k ID uživatelů bez časového limitu, budou informace o prostředku zrušeny. Pokud nechcete časový limit ID uživatelů používat, nastavte hodnotu parametru *INTERVAL* na nulu. Je-li však hodnota parametru *INTERVAL* nulová, úložiště obsazeno ID uživatelů a jejich přidružené prostředky se neuvolní, dokud nezadáte příkaz **REFRESH SECURITY** nebo **RVERIFY SECURITY** .

Vyladění této hodnoty může být důležité, pokud máte mnoho uživatelů bez jednoho uživatele. Nastavíte-li krátký časový interval a hodnoty časového limitu, budou uvolněny prostředky, které již nejsou zapotřebí.

**Poznámka:** Pokud použijete hodnoty pro *INTERVAL* nebo *TIMEOUT* jiné než výchozí nastavení, musíte znovu zadat příkaz při každém spuštění správce front. To lze provést automaticky vložení příkazu **ALTER SECURITY** do datové sady CSQINP1 pro daného správce front.

## **Aktualizace zabezpečení správce front v systému z/OS**

IBM MQ for z/OS ukládá do mezipaměti data produktu RACF pro zlepšení výkonu. Když změníte určité třídy zabezpečení, musíte aktualizovat tyto informace uložené v mezipaměti. Nepravidelně obnovujte zabezpečení z výkonnostních důvodů. Můžete se také rozhodnout aktualizovat pouze informace o zabezpečení SSL.

Když je fronta otevřena poprvé (nebo poprvé od obnovení zabezpečení), IBM MQ provede kontrolu RACF za účelem získání přístupových práv uživatele a umístí tyto informace do mezipaměti. Data v mezipaměti zahrnují ID uživatelů a prostředky, na kterých byla provedena kontrola zabezpečení. Je-li fronta znovu otevřena stejným uživatelem, přítomnost dat uložených v mezipaměti znamená, že produkt IBM MQ nemusí vydávat RACF kontroly, což zlepšuje výkonnost. Cílem akce aktualizace zabezpečení je zrušit všechny informace o zabezpečení uložené v mezipaměti a vynutit tak IBM MQ novou kontrolu nad produktem RACF. Kdykoli přidáte, změníte nebo odstraníte profil prostředků produktu RACF , který je zadřen ve třídě MQADMIN, MXADMIN, MQPROC, MXQUEUE, MXQUEUE, MXQUEUE, MQNLIST nebo MXTOPIC, nebo MXTOPIC, musíte sdělit správcům front, kteří používají tuto třídu, aby aktualizovaly informace o zabezpečení, které zadržují. Chcete-li to provést, zadejte následující příkazy:

- Příkaz RACF SETROPTS RACLIST (classname) REFRESH, který se má obnovit na úrovni RACF .
- Příkaz IBM MQ REFRESH SECURITY, který aktualizuje informace o zabezpečení uložené správcem front. Tento příkaz musí vydat každý správce front, který má přístup k profilům, které se změnily. Máte-li skupinu sdílení front, můžete použít atribut oboru příkazu k přímému zadání příkazu pro všechny správce front ve skupině.

Používáte-li generické profily v libovolné třídě produktu IBM MQ , musíte při změně, přidání nebo odstranění všech generických profilů zadat také normální příkazy pro aktualizaci produktu RACF . Příklad: SETROPTS GENERIC (název\_ třídy) OBNOVIT.

Pokud je však profil prostředků RACF přidán, změněn nebo odstraněn a prostředek, ke kterému se vztahuje, nebyl dosud zpřístupněn (proto nejsou do mezipaměti uloženy žádné informace), produkt IBM MQ použije nové informace RACF bez vydání příkazu REFRESH SECURITY.

Je-li zapnuto monitorování RACF , (například pomocí příkazu RACF RALTER AUDIT (access-pokus (audit\_access\_level)), žádné ukládání do mezipaměti se nekoná, a proto IBM MQ odkazuje přímo na prostor RACF dataspace pro každou kontrolu. Změny jsou proto okamžitě vyzvednuty a REFRESH

SECURITY není nutná pro přístup ke změnám. Můžete potvrdit, zda je monitorování RACF zapnuto, pomocí příkazu RACF RLIST. Můžete například zadat příkaz:

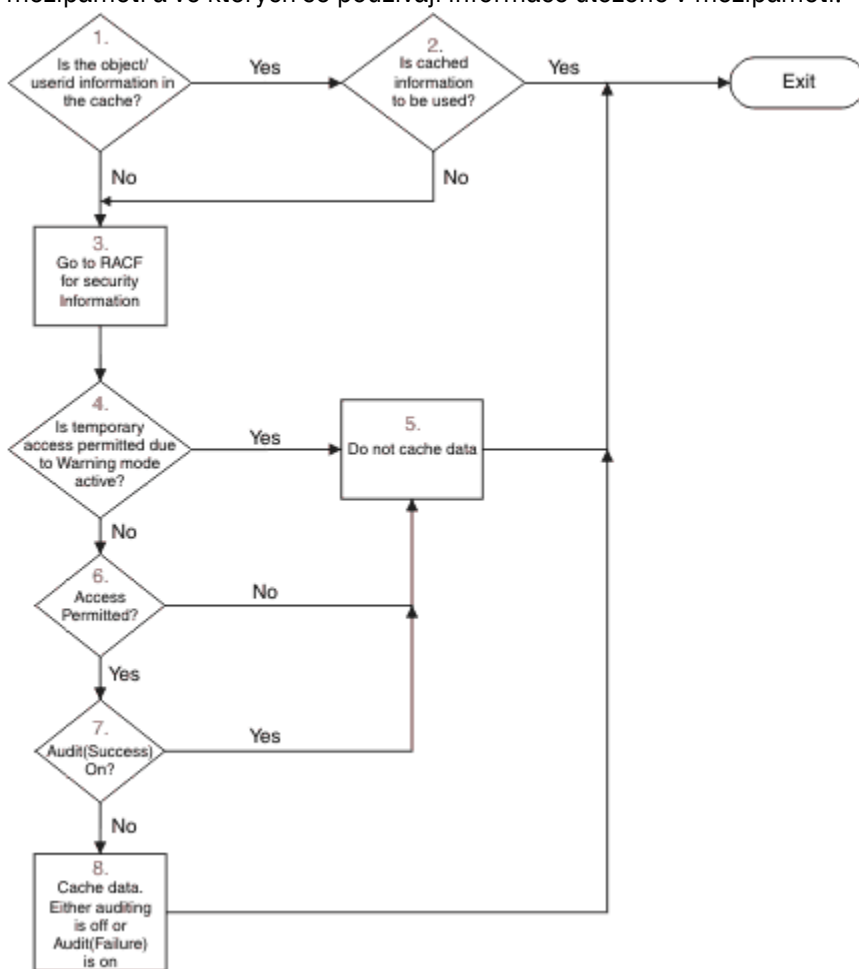
```
RLIST MQQUEUE (qmgr.SYSTEM.COMMAND.INPUT) GEN
```

a přijmout výsledky

```
CLASS      NAME
-----
MQQUEUE    QP*.SYSTEM.COMMAND.*.* (G)
           AUDITING
           -----
           FAILURES(READ)
```

To označuje, že je zapnuto auditování. Další informace naleznete v příručce *z/OS Security Server RACF Auditor's Guide* a v příručce *z/OS Security Server RACF Command Language Reference*.

Obrázek 17 na stránce 234 shrnuje situace, ve kterých se informace o zabezpečení ukládají do mezipaměti a ve kterých se používají informace uložené v mezipaměti.



Obrázek 17. Logický tok pro ukládání do mezipaměti zabezpečení produktu IBM MQ

Změníte-li nastavení zabezpečení přidáním nebo odstraněním profilů přepínače ve třídách MQADMIN nebo MXADMIN, použijte jeden z těchto příkazů k dynamickému výběru těchto změn:

- AKTUALIZOVAT ZABEZPEČENÍ (\*)
- AKTUALIZOVAT ZABEZPEČENÍ (MQADMIN)
- AKTUALIZOVAT ZABEZPEČENÍ (MXADMIN)

To znamená, že můžete aktivovat nové typy zabezpečení nebo je deaktivovat, aniž byste museli restartovat správce front.

Z výkonnostních důvodů jsou to jediné třídy ovlivněné příkazem REFRESH SECURITY. Při změně profilu ve třídách MQCONN nebo MQCMDS *není* třeba použít hodnotu REFRESH SECURITY.

**Poznámka:** Aktualizace třídy MQADMIN nebo MXADMIN není vyžadována, pokud změníte profil zabezpečení RESLEVEL.

Z výkonnostních důvodů použijte parametr REFRESH SECURITY tak často, jak je to možné, ideálně v době mimo špičku. Můžete minimalizovat počet obnov zabezpečení připojením uživatelů ke skupinám RACF, které jsou již v seznamu pro přístup k profilům IBM MQ, a nikoli k ukládání jednotlivých uživatelů do seznamů pro přístup. Tímto způsobem změníte spíše uživatele než profil prostředků. Můžete také RVERIFY SECURITY odpovídajícího uživatele místo obnovení zabezpečení.

Jako příklad REFRESH SECURITY předpokládejme, že definujete nové profily k ochraně přístupu do front začínajících řetězcem INSURANCE.LIFE ve správci front PRMQ. Použijte tyto příkazy RACF:

```
RDEFINE MQQUEUE PRMQ.INSURANCE.LIFE.** UACC(NONE)
PERMIT PRMQ.INSURANCE.LIFE.** ID(LIFEGRP) ACCESS(UPDATE)
```

Musíte zadat následující příkaz, abyste sdělili produktu RACF, že má aktualizovat informace o zabezpečení, které zadržuje, například:

```
SETROPTS RACLIST(MQQUEUE) REFRESH
```

Vzhledem k tomu, že tyto profily jsou generické, musíte produktu RACF sdělit, aby se aktualizování generických profilů pro MQQUEUE aktualizování. Příklad:

```
SETROPTS GENERIC(MQQUEUE) REFRESH
```

Pak je třeba pomocí tohoto příkazu sdělit správci front PRMQ, že se profily fronty změnily:

```
REFRESH SECURITY(MQQUEUE)
```

## Aktualizace zabezpečení SSL

Chcete-li aktualizovat zobrazení úložiště klíčů SSL uložené v mezipaměti, zadejte příkaz REFRESH SECURITY s volbou TYPE (SSL). To vám umožní aktualizovat některá nastavení SSL, aniž byste museli restartovat inicializátor kanálu.

## Zobrazení stavu zabezpečení

Chcete-li zobrazit stav přepínačů zabezpečení a dalších ovládacích prvků zabezpečení, zadejte příkaz MQSC DISPLAY SECURITY.

Na následujícím obrázku je znázorněn typický výstup příkazu DISPLAY SECURITY ALL.



```

CSQH015I +CSQ1 Security timeout = 54 MINUTES
CSQH016I +CSQ1 Security interval = 12 MINUTES
CSQH030I +CSQ1 Security switches ...
CSQH034I +CSQ1 SUBSYSTEM: ON, 'SQ05.NO.SUBSYS.SECURITY' not found
CSQH032I +CSQ1 QMGR: ON, 'CSQ1.YES.QMGR.CHECKS' found
CSQH031I +CSQ1 QSG: OFF, 'SQ05.NO.QSG.CHECKS' found
CSQH031I +CSQ1 CONNECTION: OFF, 'CSQ1.NO.CONNECT.CHECKS' found
CSQH034I +CSQ1 COMMAND: ON, 'CSQ1.NO.COMMAND.CHECKS' not found
CSQH031I +CSQ1 CONTEXT: OFF, 'CSQ1.NO.CONTEXT.CHECKS' found
CSQH034I +CSQ1 ALTERNATE USER: ON, 'CSQ1.NO.ALTERNATE.USER.CHECKS' not found
CSQH034I +CSQ1 PROCESS: ON, 'CSQ1.NO.PROCESS.CHECKS' not found
CSQH034I +CSQ1 NAMELIST: ON, 'CSQ1.NO.NLIST.CHECKS' not found
CSQH034I +CSQ1 QUEUE: ON, 'CSQ1.NO.QUEUE.CHECKS' not found
CSQH034I +CSQ1 TOPIC: ON, 'CSQ1.NO.TOPIC.CHECKS' not found
CSQH031I +CSQ1 COMMAND RESOURCES: OFF, 'CSQ1.NO.CMD.RESC.CHECKS' found
CSQ9022I +CSQ1 CSQHPDTC ' DISPLAY SECURITY' NORMAL COMPLETION

```

Obrázek 18. Typický výstup z příkazu `DISPLAY SECURITY`

Příklad ukazuje, že správce front, který odpovídal na příkaz, má subsystém, příkaz, alternativní uživatele, proces, seznam názvů a zabezpečení fronty, které jsou aktivní na úrovni správce front, nikoli však na úrovni skupiny sdílení front. Připojení, prostředek příkazu a zabezpečení kontextu nejsou aktivní. Také ukazuje, že jsou aktivní časové limity ID uživatele a že každých 12 minut správce front zkontroluje ID uživatele, která nebyla použita v tomto správci front během 54 minut, a odebere je.

**Poznámka:** Tento příkaz zobrazí aktuální stav zabezpečení. Nenutně odráží aktuální stav profilů přepínačů definovaných pro RACF nebo stav tříd RACF. Např. profily přepínače se mohly změnit od posledního restartu tohoto správce front nebo příkazu `REFRESH SECURITY`.

## Úlohy instalace zabezpečení pro produkt z/OS

Po instalaci a úpravě produktu IBM MQ autorizujte spuštěné procedury úloh pro produkt RACF, autorizujte přístup k různým prostředkům a nastavte definice RACF. Volitelně můžete konfigurovat systém pro zabezpečení SSL.

Je-li produkt IBM MQ poprvé nainstalován a upraven, je třeba provést tyto úlohy související se zabezpečením:

1. Nastavení IBM MQ datové sady a zabezpečení systému pomocí:
  - Autorizace správce front byla spuštěna-procedura úlohy xxxxMSTR a distribuovaná fronta spustila-úloha xxxxCHIN, která má být spuštěna v rámci produktu RACF.
  - Autorizování přístupu k datovým sadám správce front.
  - Autorizující přístup k prostředkům pro jména uživatelů, která budou používat správce front a obslužné programy.
  - Autorizuje přístup pro ty správce front, kteří budou používat struktury seznamu prostředku Coupling Facility.
  - Autorizuje přístup pro ty správce front, kteří budou používat produkt Db2.
2. Nastavte definice RACF pro zabezpečení produktu IBM MQ.
3. Chcete-li používat SSL (Secure Sockets Layer), připravte svůj systém k použití certifikátů a klíčů.

### **Nastavení zabezpečení datové sady produktu IBM MQ for z/OS**

Existuje mnoho typů uživatelů IBM MQ. RACF umožňuje řídit jejich přístup k datovým sadám systému.

Možné uživatele datových sad produktu IBM MQ zahrnují následující entity:

- Samotný správce front.
- Inicializátor kanálu
- Administrátoři produktu IBM MQ, kteří potřebují vytvořit datové sady produktu IBM MQ, spouštět obslužné programy a podobné úlohy.

- Programátoři aplikací, kteří potřebují používat zakladače dodávané s produktem IBM MQ, obsahují datové sady, makra a podobné prostředky.
- Žádosti zahrnující jednu nebo více z těchto položek:
  - Dávkové úlohy
  - TSO uživatelé
  - Oblasti položek CICS
  - Oblasti položek IMS
- Datové sady CSQOUTX a CSQSNAP
- Dynamické fronty SYSTEM.CSQXCMD.\*

Pro všechny tyto potenciální uživatele chraňte datové sady produktu IBM MQ pomocí produktu RACF. Musíte také řídit přístup ke všem datovým sadám 'CSQINP'.

#### *RACF autorizace spuštěných procedur úloh*

Některé datové sady produktu IBM MQ jsou určeny pro výlučné použití správce front. Pokud chráníte své datové sady produktu IBM MQ pomocí produktu RACF, musíte také autorizovat spuštěnou úlohu správce front xxxxMSTRa postup spuštění distribuované fronty úloh xxxxCHINpomocí příkazu RACF. Chcete-li to provést, použijte třídu STARTED. Alternativně můžete použít tabulku spuštěných procedur (ICHRIN03), ale pak musíte provést IPL systému z/OS , aby se změny projevíly.

Další informace najdete v příručce *z/OS Security Server RACF System Programmer's Guide*.

Identifikovaná ID uživatele produktu RACF musí mít požadovaný přístup k datovým sadám v proceduře spuštění úlohy. Například, pokud přidružíte proceduru spuštění úlohy správce front s názvem CSQ1MSTR s ID uživatele RACF QMGRCSQ1, musí mít ID uživatele QMGRCSQ1 přístup k prostředkům produktu z/OS , ke kterým má přístup správce front CSQ1 .

Také obsah pole GROUP v ID uživatele správce front musí být stejný jako obsah pole GROUP v profilu STARTED pro daného správce front. Pokud se obsah v každém poli GROUP neshoduje, pak se mu do systému nezabrání odpovídající ID uživatele. Tato situace způsobí, že produkt IBM MQ bude spuštěn s nedefinovaným ID uživatele a následně se uzavře kvůli narušení zabezpečení.

ID uživatelů produktu RACF přidružená k procedurám úlohy spuštěných úloh správce front a inicializátoru kanálu nesmí mít nastaven atribut TRUSTED.

#### *Autorizování přístupu k datovým sadám*

Datové sady produktu IBM MQ by měly být chráněny, aby žádný neautorizovaný uživatel mohl spustit instanci správce front, nebo získat přístup k datům správce front. Chcete-li to provést, použijte normální ochranu dat sady z/OS RACF .

Tabulka 62 na stránce 237 shrnuje přístup produktu RACF , který spustil proceduru úlohy správce front, k různým datovým sadám.

<i>Tabulka 62. RACF přístup k datovým sadám přidruženým ke správci front</i>	
<b>RACF přístup</b>	<b>Datové sady</b>
READ (čtení)	<ul style="list-style-type: none"> <li>• thlqual.SCSQAUTH a thlqual.SCSQANLx (kde x je jazyková písmena pro váš národní jazyk).</li> <li>• Datové sady odkazované pomocí CSQINP1, CSQINP2 a CSQXLIB v proceduře spuštěné úlohy správce front.</li> <li>• datové sady SMDS vlastněné jinými správci front ve skupině.</li> <li>• Log, BSDS a archivní datové sady protokolu pro ostatní správce front ve skupině.</li> </ul>

<i>Tabulka 62. RACF přístup k datovým sadám přidruženým ke správci front (pokračování)</i>	
<b>RACF přístup</b>	<b>Datové sady</b>
AKTUALIZOVAT	<ul style="list-style-type: none"> <li>• Všechny sady stránek a datové sady protokolu a BSDS.</li> <li>• datové sady SMDS vlastněné správcem front</li> </ul>
ALTER	<ul style="list-style-type: none"> <li>• Všechny datové sady protokolu archivace.</li> </ul>

Tabulka 63 na stránce 238 shrnuje přístup RACF , který musí mít procedura spuštěné úlohy pro distribuované řazení do front k různým datovým sadám.

<i>Tabulka 63. RACF přístup k datovým sadám přidruženým k distribuovaným frontováním</i>	
<b>RACF přístup</b>	<b>Datové sady</b>
READ (čtení)	<ul style="list-style-type: none"> <li>• thlqual.SCSQAUTH, thlqual.SCSQANLx (kde x je jazyková písmena pro váš národní jazyk) a thlqual.SCSQMVR1.</li> <li>• Datové sady knihovny LE.</li> <li>• Datové sady odkazované CSQXLIB a CSQINPX v proceduře spuštění úlohy iniciátoru kanálu.</li> </ul>
AKTUALIZOVAT	<ul style="list-style-type: none"> <li>• Datové sady CSQOUTX a CSQSNAP</li> </ul>

Další informace viz příručka *z/OS Security Server RACF Security Administrator's Guide*.

### **Nastavení zabezpečení prostředků produktu IBM MQ for z/OS**

Existuje mnoho typů uživatelů IBM MQ . Pomocí produktu RACF můžete řídit jejich přístup k prostředkům produktu IBM MQ .

Možnými uživateli prostředků produktu IBM MQ , jako jsou fronty a kanály, patří následující entity:

- Samotný správce front.
- Inicializátor kanálu
- Administrátoři produktu IBM MQ , kteří potřebují vytvořit datové sady produktu IBM MQ , spouštět obslužné programy a podobné úlohy
- Programátoři aplikací, kteří potřebují používat zakladače dodávané s produktem IBM MQ, obsahují datové sady, makra a podobné prostředky.
- Žádosti zahrnující jednu nebo více z těchto položek:
  - Dávkové úlohy
  - TSO uživatelé
  - Oblasti položek CICS
  - Oblasti položek IMS
- Datové sady CSQOUTX a CSQSNAP
- Dynamické fronty SYSTEM.CSQXCMD.\*

Pro všechny tyto potenciální uživatele chraňte prostředky produktu IBM MQ pomocí produktu RACF. Konkrétně si všimněte, že iniciátor kanálu potřebuje přístup k různým prostředkům, jak je popsáno v [“Aspekty zabezpečení pro inicializátor kanálu v systému z/OS”](#) na stránce 244, a proto musí mít ID uživatele, pod kterým je spuštěna, oprávnění pro přístup k těmto prostředkům.

Pokud používáte skupinu sdílení front, může správce front vydávat různé příkazy interně, takže ID uživatele, které používá, musí mít oprávnění k vydávání těchto příkazů. Tyto příkazy jsou:

- DEFINE, ALTER a DELETE pro každý objekt, který má QSGDISP (GROUP)

- START a STOP CHANNEL pro každý kanál, který se používá se CHLDISP (SHARED)

## **z/OS Konfigurace systému z/OS pro použití protokolu SSL (Secure Sockets Layer)**

Toto téma se používá jako příklad konfigurace produktu IBM MQ for z/OS se zabezpečením SSL pomocí příkazů produktu RACF .

Chcete-li použít zabezpečení SSL pro zabezpečení kanálu, je třeba v systému provést určité úlohy. (Podrobné informace o použití příkazů RACF pro certifikáty a úložiště klíčů (klíčové řetězce) naleznete v tématu [Práce s SSL nebo TLS v systému z/OS](#) .)

1. Vytvořte svazek klíčů v produktu RACF pro uložení všech klíčů a certifikátů pro váš systém pomocí příkazu RACDCERT RACF . Příklad:

```
RACDCERT ID(CHINUSER) ADDRING(QM1RING)
```

ID musí být buď ID uživatele adresního prostoru kanálu kanálu, nebo ID uživatele, které chcete vlastnit svazek klíčů, pokud se má jednat o sdílený svazek klíčů.

2. Vytvořte digitální certifikát pro každého správce front pomocí příkazu RACF RACDCERT.

Návěští certifikátu musí být buď hodnota atributu IBM MQ **CERTLABL** , je-li nastavena, nebo výchozí `ibmWebSphereMQ` s názvem správce front nebo skupiny sdílení front s připojeným názvem. Podrobnosti najdete v tématu [Digitální certifikáty certifikátu](#) . V tomto příkladě je to `ibmWebSphereMQM1`.

Příklad:

```
RACDCERT ID(USERID) GENCERT
SUBJECTSDN(CN('username') O('IBM') OU('departmentname') C('England'))
WITHLABEL('ibmWebSphereMQM1')
```

3. Připojte certifikát v produktu RACF k souboru svazku klíčů pomocí příkazu RACF RACDCERT. Příklad:

```
RACDCERT CONNECT(ID(USERID) LABEL('ibmWebSphereMQM1') RING(QM1RING))
CONNECT ID(CHINUSER)
```

Je také třeba připojit všechny příslušné certifikáty podepisujících subjektů (od certifikační autority) ke klíči svazku klíčů. To znamená, že všechny certifikační autority pro certifikát SSL tohoto správce front a všechny certifikační autority pro všechny certifikáty SSL, se kterými tento správce front komunikuje. Příklad:

```
RACDCERT ID(CHINUSER)
CONNECT(CERTAUTH LABEL('My CA') RING(QM1RING) USAGE(CERTAUTH))
```

4. V každém z vašich správců front použijte příkaz IBM MQ ALTER QMGR a určete úložiště klíčů, na které má správce front odkazovat. Je-li například svazek klíčů vlastněný adresním prostorem inicializátoru kanálu:

```
ALTER QMGR SSLKEYR(QM1RING)
```

nebo pokud používáte sdílený svazek klíčů:

```
ALTER QMGR SSLKEYR(userid/QM1RING)
```

kde *userid* je ID uživatele, který vlastní sdílený svazek klíčů.

5. Seznamy odvolaných certifikátů (CRL) umožňují certifikačním orgánům odvolávat certifikáty, které již nemohou být důvěryhodné. Seznamy CRL jsou uloženy na serverech LDAP. Chcete-li získat přístup na tento seznam na serveru LDAP, musíte nejprve vytvořit objekt AUTHINFO typu AUTHTYPE CRLLDAP pomocí příkazu IBM MQ DEFINE AUTHINFO. Příklad:

```
DEFINE AUTHINFO(LDAP1)  
AUTHTYPE(CRLLDAP)  
CONNNAME(ldap.server(389))  
LDAPUSER('')  
LDAPPWD('')
```

V tomto příkladu je seznam odvolaných certifikátů uložen ve veřejné oblasti na serveru LDAP, takže pole LDAPUSER a LDAPPWD nejsou nezbytná.

Dále umístěte objekt AUTHINFO do seznamu názvů pomocí příkazu IBM MQ DEFINE NAMELIST. Příklad:

```
DEFINE NAMELIST(LDAPNL) NAMES(LDAP1)
```

Nakonec přiřadíte seznam názvů k jednotlivým správcům front pomocí příkazu IBM MQ ALTER QMGR. Příklad:

```
ALTER QMGR SSLCRLNL(LDAPNL)
```

6. Set up your queue manager to run SSL calls, using the IBM MQ ALTER QMGR command. Toto definuje podúlohy serveru, které obsluhují pouze volání SSL, což ponechá normální dispečery pokračovat ve zpracování jako normální, aniž by to bylo ovlivněno žádným voláním SSL. Musíte mít alespoň dva z těchto podúloh. Příklad:

```
ALTER QMGR SSLTASKS(8)
```

Tato změna se projeví až po restartování inicializátoru kanálu.

7. Uvedte specifikaci šifry, která má být použita pro každý kanál, pomocí příkazu IBM MQ DEFINE CHANNEL nebo ALTER CHANNEL. Příklad:

```
ALTER CHANNEL(LDAPCHL)  
CHLTYPE(SDR)  
SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA)
```

Oba konce kanálu musí uvádět stejnou specifikaci šifry.

## Správa záznamů ověření kanálu ve skupině sdílení front

Záznamy ověření kanálu se vztahují na správce front, kterého jsou vytvořeny, nebudou sdíleny v rámci skupiny sdílení front. Proto jsou-li všichni správci front ve skupině sdílení front povinni mít stejná pravidla, je třeba provést některé řízení tak, aby byla zachována konzistence všech pravidel.

1. Vždy přidejte volbu CMDSCOPE (\*) do všech příkazů SET CHLAUTH . Tento příkaz odešle příkaz všem spuštěným správcům front ve skupině sdílení front.
2. Použijte příkaz DISPLAY CHLAUTH s volbou CMDSCOPE (\*) a potom analyzujte odezvy, abyste zjistili, zda jsou záznamy stejné od všech správců front. Je-li nalezena nekonzistence, lze zadat příkaz SET CHLAUTH obsahující stejné pravidlo s CMDSCOPE (\*) nebo CMDSCOPE (*qmgr-name*).
3. Přidejte člena do zřetězení CSQINP2 správce front (viz [Inicializační příkazy](#)), které mají úplnou sadu pravidel. Ty budou načteny jako součást procesu inicializace správce front. Pokud příkaz SET CHLAUTH používá příkaz ACTION(ADD), bude pravidlo přidáno pouze v případě, že neexistuje. Použití ACTION(REPLACE) nahradí existující pravidlo, pokud již existuje, nebo jej přidat, pokud se tak nestane. Stejný člen by pak mohl být umístěn ve zřetězení CSQINP2 všech správců front ve skupině sdílení front.
4. Chcete-li extrahovat pravidla z jednoho správce front pomocí volby MAKEDEF nebo MAKEREP, použijte obslužný program CSQUTIL (viz část [Vydávání příkazů do IBM MQ \(COMMAND\)](#)). Pak přehrajte výstup pomocí CSQUTIL do cílového správce front.

### Související pojmy

#### Záznamy ověření kanálu

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

## Aspekty auditování v systému z/OS

Pro provádění auditu zabezpečení správce front jsou k dispozici standardní ovládací prvky auditování produktu RACF. Produkt IBM MQ neshromažďuje žádné statistické údaje zabezpečení. Jediné statistiky jsou ty, které mohou být vytvářeny auditováním.

Auditování RACF může být založeno na:

- ID uživatelů
- Třídy prostředků
- Profily

Další informace najdete v příručce *z/OS Security Server RACF Auditor's Guide*.

**Poznámka:** Auditování degraduje výkon, čím více auditování implementujete, tím více je degradováno. Jedná se také o úvahu pro použití volby VAROVÁNÍ RACF.

### **Audit RESLEVEL**

Pomocí systémového parametru RESAUDIT můžete řídit produkci záznamů auditu RESLEVEL. RACF OBECNÉ záznamy auditu jsou vytvořeny.

Vytvořte záznamy auditu RESLEVEL pomocí nastavení systémového parametru RESAUDIT na hodnotu YES. Je-li parametr RESAUDIT nastaven na NO, záznamy auditu se nevytvoří. Další podrobnosti o nastavení tohoto parametru naleznete v tématu [Použití CSQ6SYSP](#).

Je-li volba RESAUDIT nastavena na hodnotu YES, nebudou při kontrole RESLEVEL při kontrole RESLEVEL provedeny žádné běžné záznamy auditu RACF, aby bylo vidět, jaký přístup má ID uživatele adresního prostoru k profilu hlq.RESLEVEL. Místo toho IBM MQ požaduje, aby RACF vytvořil GENERAL záznam auditu (událost číslo 27). Tyto kontroly jsou prováděny pouze v době připojení, takže náklady na výkon jsou minimální.

Záznamy obecného auditu IBM MQ můžete hlásit pomocí zapisovacího programu sestav RACF (RACFRW). K hlášení přístupu RESLEVEL můžete použít následující příkazy RACFRW:

```

RACFRW
SELECT PROCESS
EVENT GENERAL
LIST
END

```

Ukázková sestava z RACFRW, kromě polí *Date*, *Time* a *SYSID*, je zobrazena v Obrázek 19 na stránce 242.

```

RACF REPORT - LISTING OF PROCESS RECORDS                                PAGE 4
E
V Q
E U
*JOB/USER *STEP/  --TERMINAL--  N A
NAME      GROUP   ID      LVL  T  L
WS21B    MQMGRP IGJZM000  0   27 0  JOBID=(WS21B 05.111 09:44:57),USERDATA=(
TRUSTED  USER          AUTH=(NONE),REASON=(NONE)
SESSION=TSOLOGON,TERMINAL=IGJZM000,
LOGSTR='CSQH RESLEVEL CHECK PERFORMED AGAINST
PROFILE(QM66.RESLEVEL),
CLASS(MQADMIN), ACCESS EQUATES TO
(CONTROL)',RESULT=SUCCESS,MQADMIN

```

Obrázek 19. Ukázkový výstup ze souboru RACFRW se zobrazením obecných záznamů auditu RESLEVEL

Při kontrole dat LOGSTR v tomto ukázkovém výstupu vidíte, že uživatel TSO WS21B má přístup CONTROL k QM66.RESLEVEL. To znamená, že všechny kontroly zabezpečení prostředků jsou vynechány, když uživatel WS21B má přístup k prostředkům QM66.

Další informace o použití příkazu RACFRW naleznete v příručce *z/OS Security Server RACF Auditor's Guide*.

## Přizpůsobení zabezpečení

Chcete-li změnit způsob zabezpečení produktu IBM MQ, je třeba provést toto nastavení prostřednictvím uživatelské procedury SAF (ICHRFR00) nebo skončit ve správci externích zabezpečení.

Další informace o uživatelských procedurách produktu RACF naleznete v příručce *z/OS Security Server RACROUTE Macro Reference*.

**Poznámka:** Protože program IBM MQ optimalizuje volání do ESM, požadavky RACROUTE nemusí být prováděny například při každém otevření určité fronty konkrétním uživatelem.

## Zprávy o narušení zabezpečení v systému z/OS

Narušení zabezpečení je označeno návratovým kódem MQRC\_NOT\_AUTHORIZED v aplikačním programu nebo prostřednictvím zprávy v protokolu úlohy.

Návratový kód operace MQRC\_NOT\_AUTHORIZED může být vrácen do aplikačního programu z následujících důvodů:

- Uživateli není dovoleno připojit se ke správci front. V takovém případě obdržíte zprávu ICH408I v protokolu úlohy Batch/TSO, CICS nebo IMS.
- Přihlášení uživatele do správce front se nezdařilo, protože například ID uživatele úlohy není platné nebo je to vhodné, nebo ID uživatele úlohy nebo alternativní ID uživatele není platné. Jedno nebo více z těchto ID uživatelů nemusí být platné, protože byly odebrány nebo odstraněny. V tomto případě získáte zprávu ICHxxxx a případně zprávu IRRxxxx v protokolu úlohy správce front, kde došlo k selhání při přihlášení. Příklad:

```

ICH408I USER(NOTDFND ) GROUP( ) NAME(???)

```

- Byl požadován alternativní uživatel, ale ID uživatele úlohy nebo úlohy nemá přístup k alternativnímu ID uživatele. Pro toto selhání obdržíte zprávu o narušení v protokolu úlohy příslušného správce front.
- Volba kontextu byla použita nebo je odvozena z otevření přenosové fronty pro výstup, ale ID uživatele úlohy nebo případně úloha nebo alternativní ID uživatele nemá přístup k volbě kontextu. V takovém případě je do protokolu úlohy příslušného správce front vložena zpráva o narušení.
- Neautorizovaný uživatel se pokusil o přístup k zabezpečenému objektu správce front, například k frontě. V tomto případě je do protokolu úlohy příslušného správce front vložena zpráva ICH408I pro narušení. Toto porušení může být způsobeno úlohou nebo, je-li to vhodné, úlohou nebo alternativním ID uživatele.

Zprávy o narušení pro zabezpečení příkazů a zabezpečení prostředků příkazů lze také najít v protokolu úlohy správce front.

Pokud zpráva o narušení ICH408I zobrazuje název úlohy správce front a nikoli ID uživatele, je obvykle výsledkem prázdného alternativního ID uživatele. Příklad:

```
ICH408I JOB(MQS1MSTR) STEP(MQS1MSTR)
      MQS1.PAYROLL.REQUEST CL(MQQUEUE)
      INSUFFICIENT ACCESS AUTHORITY
      ACCESS INTENT(UPDATE ) ACCESS ALLOWED(NONE )
```

Můžete zjistit, komu je povoleno používat prázdná alternativní ID uživatelů, a to tak, že zkontrolujete seznam pro přístup k profilu MQADMIN hlq.ALTERNATE.USER.-BLANK-.

Zprávu o narušení ICH408I lze také vygenerovat příkazem:

- Příkaz odesílaný do vstupní fronty příkazového řádku bez kontextu. Uživatelské programy, které zapisují do vstupní fronty systémových příkazů, by vždy měly používat volbu kontextu. Další informace viz [“Profily pro zabezpečení kontextu”](#) na stránce 202.
- Když úloha přistupující k prostředku IBM MQ nemá přidružené ID uživatele nebo pokud adaptér IBM MQ nemůže extrahovat ID uživatele z prostředí adaptéru.

Zprávy o narušení mohou být vydávány také v případě, že používáte skupinu sdílení front i zabezpečení na úrovni správce front. Můžete získat zprávy označující, že nebyl nalezen žádný profil na úrovni správce front, ale stále mu bude udělen přístup z důvodu profilu skupiny sdílení front.

```
ICH408I JOB(MQS1MSTR) STEP(MQS1MSTR)
      MQS1.PAYROLL.REQUEST CL(MQQUEUE)
      PROFILE NOT FOUND - REQUIRED FOR AUTHORITY CHECKING
      ACCESS INTENT(UPDATE ) ACCESS ALLOWED(NONE )
```

## Co dělat, pokud je přístup povolen nebo nepovolen nesprávně

Kromě kroků podrobně popsanych v příručce *z/OS Security Server RACF Security Administrator's Guide* použijte tento kontrolní seznam, pokud se zdá, že přístup k prostředku je nesprávně řízen.

- Jsou profily přepínačů správně nastaveny?
  - Je RACF aktivní?
  - Jsou třídy IBM MQ RACF instalovány a aktivní?
    - Chcete-li to zkontrolovat, použijte příkaz RACF SETROPTS LIST.
  - Chcete-li zobrazit aktuální stav přepínače ze správce front, použijte příkaz IBM MQ DISPLAY SECURITY.
  - Zkontrolujte profily přepínačů ve třídě MQADMIN.



- Pro tento příkaz použijte příkazy RACF , SEARCH a RLIST.
- Znovu zkontrolujte profily přepínačů RACF zadáním příkazu IBM MQ REFRESH SECURITY (MQADMIN).
  - Změnil se profil prostředků RACF ? Má se například změněn univerzální přístup na profil nebo je změněn seznam přístupů profilu?
    - Je profil generický?
      - Je-li tomu tak, zadejte příkaz RACF SETROPTS GENERIC (název\_třídy) OBNOVIT.
    - Aktualizovali jste zabezpečení tohoto správce front?
      - Je-li to nutné, zadejte příkaz RACF SETROPTS RACLIST (název\_třídy) OBNOVIT.
      - Je-li to nutné, zadejte příkaz IBM MQ REFRESH SECURITY (\*).
  - Změnila se definice RACF uživatele? Například, byl uživatel připojen k nové skupině nebo má oprávnění k přístupu uživatele zrušeno oprávnění?
    - Ověřili jste uživatele zadáním příkazu IBM MQ RVERIFY SECURITY (userid)?
  - Jsou v důsledku RESLEVEL vynechány kontroly zabezpečení?
    - Zkontrolujte přístup ID uživatele s připojením k profilu RESLEVEL. Použijte záznamy auditu RACF , abyste určili, na kterou hodnotu RESLEVEL je nastavena.
    - V případě kanálů pamatujte na to, že úroveň přístupu, kterou ID uživatele iniciátoru kanálu má na RESLEVEL, zdědí všechny kanály, takže úroveň přístupu, jako např. ALTER, která způsobí, že všechny kontroly budou vynechány, způsobí, že budou všechny kanály vynechány pro všechny kanály.
    - Pokud spouštíte produkt CICS, zkontrolujte nastavení RESESEC transakce.
    - Pokud byla při připojení uživatele změněna hodnota RESLEVEL, musí se před novým nastavením RESLEVEL znovu odpojit a znovu připojit.
  - Používáte skupiny sdílení front?
    - Používáte-li skupinu sdílení front i úroveň zabezpečení správce front, zkontrolujte, zda jste definovali všechny správné profily. Není-li profil správce front definován, odešlo se do protokolu zpráva s informací o tom, že profil nebyl nalezen.
    - Použili jste kombinaci nastavení přepínače, která není platná, takže byla nastavena úplná kontrola zabezpečení?
    - Potřebujete definovat přepínače zabezpečení, chcete-li přepsat některá nastavení skupiny sdílení front pro správce front?
    - Má profil na úrovni správce front přednost před profilem skupiny sdílení front?

## Aspekty zabezpečení pro inicializátor kanálu v systému z/OS

Pokud používáte zabezpečení na úrovni prostředků v distribuovaném prostředí řazení do fronty, potřebuje adresní prostor Inicializátor kanálu odpovídající přístup k různým prostředkům produktu IBM MQ . K vytvoření algoritmu ochrany heslem můžete použít program Integrated Cryptographic Support Facility (ICSF).

## Použití zabezpečení prostředků

Pokud používáte zabezpečení prostředků, zvažte následující body, pokud používáte distribuované ukládání do fronty:

### systemových front

Adresní prostor inicializátoru kanálu potřebuje přístup RACF UPDATE k systémovým frontám uvedeným v seznamu “Zabezpečení systémové fronty” na stránce 191a ke všem cílovým frontám uživatele a frontám nedoručených zpráv (viz “Zabezpečení fronty nedoručených zpráv” na stránce 190).

### Přenosové fronty

Adresní prostor inicializátoru kanálu vyžaduje přístup ALTER ke všem přenosovým frontám uživatele.

## **zabezpečení kontextu**

ID uživatele kanálu (a ID uživatele MCA, je-li zadán) potřebují RACF CONTROL přístup k profilům hlq.CONTEXT.queueaname ve třídě MQADMIN. V závislosti na profilu RESLEVEL může ID uživatele kanálu také potřebovat CONTROL přístup k těmto profilům.

Všechny kanály vyžadují přístup CONTROL k souboru MQADMIN hlq.CONTEXT. profil fronty nedoručených zpráv. Všechny kanály (ať již iniciující nebo odpovídající) mohou generovat sestavy a v důsledku toho potřebují přístup CONTROL k profilu hlq.CONTEXT.reply-q .

Kanály SENDER, CLUSSDR a SERVER vyžadují přístup CONTROL k profilům hlq.CONTEXT.xmit-queue-name , protože zprávy mohou být vloženy do přenosové fronty, aby se kanál mohl ukončit postupně.

**Poznámka:** Pokud má ID uživatele kanálu nebo skupina RACF , ke které je připojeno ID uživatele kanálu, přístup CONTROL nebo ALTER k souboru hlq.RESLEVEL, nejsou pro iniciátor kanálu nebo některé jeho kanály žádné kontroly prostředků.

Další informace viz [“Profily pro zabezpečení kontextu”](#) na stránce 202 [“RESLEVEL a připojení inicializátoru kanálu”](#) na stránce 220 a [“ID uživatele pro kontrolu zabezpečení”](#) na stránce 222 .

## **CSQINPX**

Pokud používáte vstupní datovou sadu CSQINPX, pak iniciátor kanálu také potřebuje přístup READ ke CSQINPX a přístup UPDATE k datové sadě CSQOUTX a dynamické fronty SYSTEM.CSQXCMD. \*

## **Zabezpečení připojení**

Požadavky na připojení adresního prostoru inicializátoru kanálu používají typ připojení CHIN, pro který musí být nastaveno odpovídající zabezpečení přístupu, viz [“Profily zabezpečení připojení pro inicializátor kanálu”](#) na stránce 185.

## **Datové sady**

Adresní prostor inicializátoru kanálu potřebuje odpovídající přístup k datovým sadám správce front, viz [“Autorizování přístupu k datovým sadám”](#) na stránce 237.

## **Příkazy**

Příkazy s distribuovanými frontami (například DEFINE CHANNEL, START CHINIT, START LISTENER a další kanálové příkazy) musí mít nastaven odpovídající sadu zabezpečení příkazů, viz [Tabulka 47](#) na stránce 205.

Pokud používáte skupinu sdílení front, iniciátor kanálu může interně vydat různé příkazy, takže ID uživatele, které používá, musí být autorizováno k vydávání těchto příkazů. Tyto příkazy jsou START a STOP CHANNEL pro každý kanál, který se používá se CHLDISP (SHARED).

Pokud PSMODE správce front není VYPNUTÝ, musí mít inicializátor kanálu přístup READ k příkazu DISPLAY PUBSUB.

## **Zabezpečení kanálu**

Kanály, zejména zásobníky a připojení k serveru, vyžadují nastavení zabezpečení. Další informace naleznete v dokumentu [“ID uživatele pro kontrolu zabezpečení”](#) na stránce 222 .

K zajištění zabezpečení na kanálech můžete také použít protokoly TLS (Transport Layer Security) nebo SSL (Secure Sockets Layer). Další informace o použití TLS a SSL s produktem IBM MQ viz [“Protokoly zabezpečení SSL a TLS v produktu IBM MQ”](#) na stránce 22 .

Další informace o zabezpečení připojení k serveru najdete v příručce [“Řízení přístupu pro klienty”](#) na stránce 83 .

## **ID uživatelů**

ID uživatelů popsaná v tématech [“ID uživatele použitá inicializátorem kanálu”](#) na stránce 225 a [“ID uživatelů použitá agentem front v rámci skupiny”](#) na stránce 229 potřebují následující přístup:

- RACF UPDATE access to the appropriate destination queues and the dead-letter queue
- RACF CONTROL přístup k profilu produktu hlq . CONTEXT . queueaname , pokud se provádí kontrola kontextu na přijímači.
- Přiměřený přístup k souboru hlq.ALTERNATE.USER.userid , které mohou potřebovat použít.
- Pro klienty je vhodný přístup RACF k prostředkům, které mají být použity.

## Zabezpečení APPC

Používáte-li přenosový protokol LU 6.2 , nastavte odpovídající zabezpečení APPC. (Například použijte třídu APPCLU RACF .) Informace o nastavení zabezpečení pro APPC naleznete v následujících příručkách:

- *z/OS V1R2.0 Plánování MVS: Správa APPC*
- Publikace *Multiplatform APPC Configuration Guide*, publikace IBM Redbooks

Odchozí přenosy používají volbu protokolu APPC "SECURITY (SAME)" . V důsledku toho je ID uživatele adresního prostoru iniciátoru kanálu a jeho výchozí profil ( RACF GROUP) přenášena po síti k příjemci s indikátorem, že ID uživatele již bylo ověřeno (ALREADYV).

Je-li přijímající strana také z/OS, ID uživatele a profil jsou ověřeny pomocí APPC a ID uživatele se předkládá k přijímacímu kanálu a používá se jako ID uživatele kanálu.

V prostředí, ve kterém správce front používá APPC ke komunikaci s jiným správcem front ve stejném nebo v jiném systému z/OS , je třeba zajistit, aby:

- Definice VTAM pro komunikující LU určuje SETACPT (ALREADYV).
- Existuje profil RACF APPCLU pro připojení mezi jednotkami LU, které uvádí CONVSEC (ALREADYV)

## Změna nastavení zabezpečení

Je-li úroveň přístupu RACF , která má ID uživatele kanálu nebo jméno uživatele MCA, změněna, projeví se tato změna pouze pro nové obslužné rutiny objektů (tj. nové MQOPEN ) pro cílovou frontu. Časy, kdy jsou otevřené fronty MCAa a zavírají fronty; pokud je kanál již spuštěn, když se provádí taková změna přístupu, může agent MCA pokračovat v vkládání zpráv do cílové fronty s použitím existujícího zabezpečeného přístupu k ID uživatelů, nikoli k aktualizovanému zabezpečovanému přístupu. Zastavení a restartování kanálů k vynucení aktualizované úrovně přístupu se tomuto scénáři vyhýbá.

## automatický restart

Pokud k restartování inicializátoru kanálu používáte produkt z/OS Automatic Restart Manager (ARM), musí být ID uživatele přidruženého k adresnímu prostoru XCFAS autorizováno pro zadání příkazu IBM MQ START CHINIT.

## Použití programu ICSF (Integrated Cryptographic Service Facility)

Inicializátor kanálu může použít službu ICSF k vygenerování náhodného čísla při zavedení algoritmu ochrany heslem pro zamaskování hesel procházejících přes kanály klienta, pokud se nepoužívá SSL/TLS. Proces generování náhodného čísla se nazývá *entropie*.

Pokud jste nainstalovali funkci z/OS , ale nespustili jste ICSF, zobrazí se zpráva [CSQX213E](#) a inicializátor kanálu používá STCK pro entropii.

Zpráva CSQX213E vás varuje, že algoritmus ochrany heslem není tak zabezpečený, jak by mohl být. Můžete však pokračovat ve svém procesu. V běhovém prostředí není žádný jiný dopad.

Pokud nemáte nainstalovanou funkci produktu z/OS , bude inicializátor kanálu automaticky používat STCK.

### Notes:

1. Použití ICSF pro entropii generuje více náhodných sekvencí než použití STCK.
2. Pokud spustíte ICSF, musíte restartovat inicializátor kanálu.
3. ICSF se požaduje pro určité CipherSpecs. Pokud se použije některou z těchto CipherSpecs a nemáte-li nainstalované služby ICSF, obdržíte zprávu [CSQX629E](#).

## Zabezpečení klastrů správců front v systému z/OS

Aspekty zabezpečení pro klastry jsou stejné pro správce front a kanály, které nejsou klastrované. Inicializátor kanálu potřebuje přístup k některým dalším systémovým frontám a některé další příkazy potřebují odpovídající sadu zabezpečení.

Můžete použít ID uživatele MCA, záznamy ověření kanálu, SSL nebo TLS a uživatelské procedury zabezpečení pro ověření kanálů klastru (stejně jako u konvenčních kanálů). Záznamy ověření kanálu nebo uživatelská procedura zabezpečení související s přijímacím kanálem klastru musí zkontrolovat, zda má vzdálený správce front povolen přístup k frontám klastru správce front serveru. Můžete začít používat podporu klastrů produktu IBM MQ, aniž byste změnili existující zabezpečení přístupu k frontě. Musíte však povolit ostatním správcům front v klastru, aby zapisoval do systému `SYSTEM.CLUSTER.COMMAND.QUEUE`, pokud se mají připojit ke klastru.

Podpora klastrů produktu IBM MQ neposkytuje mechanismus k omezení člena klastru pouze na roli klienta. V důsledku toho si musíte být jisti, že důvěřujete všem správcům front, které povolíte do klastru. Pokud některý správce front v klastru vytvoří frontu s určitým názvem, může pro tuto frontu přijímat zprávy bez ohledu na to, zda aplikace vkládá zprávy do této fronty nebo ne.

Chcete-li omezit členství klastru, proveďte stejnou akci, jakou byste měli provést, abyste zabránili připojení správců front k přijímacím kanálům. Členství v klastru omezíte tím, že použijete záznamy ověření kanálu nebo napíšete uživatelský program zabezpečení do přijímacího kanálu. Můžete také napsat ukončovací program, který zabráni neoprávněným správcům front zapisovat do `SYSTEM.CLUSTER.COMMAND.QUEUE`.

**Poznámka:** Doporučuje se, aby aplikace neotvířely `SYSTEM.CLUSTER.TRANSMIT.QUEUE` přímo. Také se nedoporučuje povolovat aplikaci, aby přímo otevřela jakoukoli jinou přenosovou frontu.

Používáte-li zabezpečení prostředků, zvažte kromě aspektů obsažených v produktu “Aspekty zabezpečení pro inicializátor kanálu v systému z/OS” na stránce 244 následující body:

#### **systemových front**

Inicializátor kanálu potřebuje RACF ALTER pro přístup k následujícím frontám systému:

- `SYSTEM.CLUSTER.COMMAND`
- `SYSTEM.CLUSTER.TRANSMIT.QUEUE`.

a přístup `UPDATE` k `SYSTEM.CLUSTER.REPOSITORY.QUEUE`

Potřebuje také přístup `READ` k libovolným seznamům názvů, které se používají pro klastrování.

#### **Příkazy**

Nastavte odpovídající zabezpečení příkazu (jak je popsáno v tématu Tabulka 47 na stránce 205). v případě příkazů podpory klastru (`REFRESH` a `RESET CLUSTER`, `SUSPEND` a `RESUME QMGR`).

## **Aspekty zabezpečení pro použití produktu IBM MQ s produktem CICS**

Adaptér CICS poskytuje informace pro IBM MQ pro použití v zabezpečení.

Adaptér CICS poskytuje následující informace pro IBM MQ speciálně pro použití v zabezpečení produktu IBM MQ :

- Zda je zabezpečení na úrovni prostředků CICS aktivní pro tuto transakci, jak je uvedeno v operandu `RESSEC` nebo `RSLC` definice `RDO TRANSACTION`.
- ID uživatele.

Pro terminálové úlohy, ke kterým se uživatel nepřihlásil, je ID uživatele CICS ID uživatele přidruženého k terminálu a je buď:

- Předvolené ID uživatele CICS, jak je uvedeno v parametru `CICS DFLTUSER SIT`
- Přednastavené ID uživatele zabezpečení zadané v definici terminálu

U neterminálových úloh se adaptér CICS pokouší získat ID uživatele s příkazem `EXEC CICS ASSIGN`. Je-li tento pokus neúspěšný, pokusí se adaptér získat ID uživatele `EXEC CICS INQUIRE TASK`. Je-li zabezpečení aktivní v produktu CICS a transakce nepřipojená k terminálu je definována s parametrem `CMDSEC (YES)`, adaptér CICS předá ID uživatele prázdné místo produktu IBM MQ.

Další informace o aspektech zabezpečení naleznete v následujících tématech:

- Zabezpečení pro adaptér CICS-IBM MQ.
- Zabezpečení pro most CICS-IBM MQ.

## **Řízení zabezpečení CICS transakcí dodaných produktem IBM MQ**

Pokud chcete, aby uživatel spravoval adaptér CICS , udělte uživateli oprávnění k určitým transakcím.

Transakce CKTI a CKAM jsou navrženy tak, aby byly spuštěny bez terminálu; žádný uživatel by neměl mít přístup k těmto transakcím. Tyto transakce jsou příklady toho, co *CICS RACF Security Guide* volá "transakce kategorie 2". Informace o tom, jak nastavit tyto transakce v produktu CICS a RACF, naleznete v informacích o transakcích kategorie 2 v příručce *CICS RACF Security Guide*.

Pokud chcete, aby uživatel spravoval adaptér CICS , musíte udělit uživateli oprávnění k těmto transakcím:

CKQC	Řídí funkce adaptéru CICS .
CKBM	Řídí funkce adaptéru CICS .
CKRT	Řídí funkce adaptéru CICS .
CKCN	Připojit
CKSD.	Odpojit
CIKRY	Statistika
CKDP	Celá obrazovka
CKDL	Zobrazení režimu linky
CKSQ	CKTI SPUŠTĚNÍ/ZASTAVENÍ

Je-li to nutné, můžete omezit přístup ke specifickým funkcím adaptéru. Chcete-li například uživatelům umožnit zobrazení stavu adaptéru prostřednictvím celoobrazovkového rozhraní, ale nic jiného, dejte jim přístup pouze k CKQC, CKBM, CKRT a CKDP.

Definujte tyto transakce na CICS s RESESEC (NO) a CMDSEC (NO). Další informace naleznete v příručce *CICS RACF Security Guide*.

### **ID uživatele adaptéru CICS**

ID uživatele přidružené k adaptéru CICS je transakce iniciátoru úlohy dodané s produktem IBM MQCKTI. To má řadu důsledků.

### **Kontrola ID uživatele pro prostředky produktu IBM MQ během PLTPI a PLTSD**

Pokud se k prostředku IBM MQ přistupuje v průběhu fáze PLTPI CICS , ID uživatele předané produktu IBM MQ je prázdné. Pokud se k prostředku IBM MQ přistupuje během fáze PLTSD CICS , ID uživatele předané uživateli IBM MQ je ID uživatele přidružené k transakci vypnutí.

Je-li CKTI spuštěn během fáze PLTPI CICS , je ID uživatele CKTI úlohou CICS sysidnt. To znamená, že ID uživatele se stejným názvem jako CICS sysidnt musí být definováno a udělen přístup k požadovaným prostředkům produktu IBM MQ , například inicializační fronty.

### **ID uživatele terminálu**

Je-li CKTI spuštěn z terminálu z transakce CKQC nebo uživatelem napsaného programu, který odkazuje na CSQCSSQ, ID uživatele, které CKTI používá, je stejné jako ID uživatele terminálu, který spustil CKTI.

### **Automatizace spouštění CKTI**

Chcete-li automatizovat spouštění CKTIs pod specifickým ID uživatele, můžete použít produkt pro automatizaci, například Tivoli NetView for z/OS. Můžete ji použít k přihlášení na konzolu CICS a vydat příkaz STARTCKTI.

Můžete také použít přednastavené terminály zabezpečení, které byly definovány pro emulaci terminálu CRLP, se sekvenčním vstupem do terminálu obsahujícím příkaz CKQC STARTTCKTI.

However, when the CICS adapter alert monitor reconnects CICS to IBM MQ, after, for example, an IBM MQ restart, only the CKTI specified at the initial IBM MQ connection is restarted. Musíte zautomatizovat spouštění jakýchkoli extra CKTIs sami.

## Rozmnožení ID uživatele CKTI na další transakce CICS

Pokud CKTI spustí další transakce CICS, například agenty MCA (Message Channel Agent) nebo uživatelem napsané CICS aplikace, je ID uživatele CKTI šířeno do těchto aplikací. Je-li například CKTI spuštěn pod ID uživatele *USERNAME* a vyskytne se událost spouštěče, která vyžaduje spuštění transakce odesílatele MCA, *TRNA*, bude transakce *TRNA* také spuštěna pod ID uživatele *USERNAME*. ID uživatele *USERNAME* proto musí mít přístup k požadované přenosové frontě.

## Aspekty zabezpečení pro produkt CICS bridge

Když spustíte CICS bridge, můžete uvést úroveň ověření, které chcete provést.

Je-li to požadováno, most zkontroluje ID uživatele a heslo extrahované ze zprávy požadavku IBM MQ před spuštěním programu CICS uvedeného ve zprávě požadavku. Správce front používá externího správce zabezpečení (ESM) (například RACF), abyste mohli provést ověření. Proto musí být ID uživatele ve zprávě požadavku definovány na ESM.

### Poznámka:

1. Pokud jste nezauřčili ID uživatele v deskriptoru zpráv (MQMD) nebo heslo v záhlaví CICS bridge (MQCIH) zprávy, úloha mostu se spustí s úrovní LOCAL ověření, a to i v případě, že jste spustili monitor mostu s jinou volbou ověření.
2. Volby, které obsahují ověření hesla (nebo PassTicket), vyžadují k poskytnutí MQCIH. Další informace o záhlaví MQCIH viz [záhlaví MQCIH- CICS bridge](#).
3. Ověření PassTicket se provádí pomocí služeb produktu IBM MQ, nikoli EXEC CICS VERIFY, protože služba CICS nepřijímá identifikátor APPLID.

Úroveň ověření, kterou můžete použít, je popsána pomocí následujících klíčových slov:

### LOKÁLNÍ

Toto je výchozí hodnota. Programy produktu CICS spuštěné úlohou mostu jsou spuštěny s ID uživatele CICS DFLTUSER, takže jsou spuštěny spolu s oprávněním asociovaným s tímto ID uživatele. Nekontroluje se ID uživatele nebo hesla. Je-li spuštěn program CICS, který se pokouší o přístup k chráněným prostředkům, pravděpodobně se nezdaří.

### IDENTIFIKOVAT

Spustíte-li úlohu monitoru s volbou IDENTIFY authentication, spustí se úloha mostu s ID uživatele uvedeným ve zprávě (MQMD). CICS programy spuštěné funkcí mostu s ID uživatele z deskriptoru MQMD. Nekontroluje se žádná kontrola hesla, ID uživatele je považováno za důvěryhodné.

### VERIFY\_UOW

Pokud MQMD.PutApplType je nastaven na hodnotu MQAT\_NO\_CONTEXT, je použito ID uživatele DFLTUSER produktu CICS, jako pro volbu ověření LOCAL. Jinak monitor mostu zkontroluje ID uživatele (v MQMD) a heslo (v souboru CIH) před spuštěním úlohy mostu a programy CICS spuštěné pomocí mostu s ID uživatele extrahovaným z MQMD. Je-li ID uživatele nebo heslo neplatné, požadavek selže s návratovým kódem MQCRC\_SECURITY\_ERROR. Následné zprávy zpracované touto transakcí se nekontrolují.

Úlohy mostu, které nelze spustit kvůli selhání zabezpečení, se znovu pokusí, pokud je zadán ROUTEMEMM=N (výchozí). Je-li však parametr ROUTEMEMM=Y zadán, jsou zprávy mostu vloženy do fronty nedoručených zpráv.

### VERIFY\_VŠE

Tato hodnota je stejná jako VERIFY\_UOW, kromě toho, že úloha mostu kontroluje ID uživatele a heslo v každé zprávě. Tato volba není použitelná pro transakce 3270 při použití produktu CICS starší než CICS Transaction Server verze 2, vydání 2.

PassTicket lze použít místo hesla, abyste se vyhnuli nutnosti zadávat hesla ve zprávách (viz příručka Security Server RACF System Programmer's Guide). Při generování PassTicket musí být zadáno APPLID.

Používáte-li jediný monitor mostu, je APPLID CICS APPLID, pokud nebyla při spuštění mostu zadána jiná hodnota. Používáte-li pro frontu více monitorů mostu, je třeba určit ID APPLID, které má být použito, pomocí parametru PASSTKTA= *ID\_aplikace* při spuštění mostu.

Pokud jste nezadali ID uživatele ve zprávě nebo jste neuvedli heslo, spustí se program CICS spuštěný CICS bridge s ID uživatele nastaveným na ID uživatele, které se používá ke spuštění monitoru mostu, bez ohledu na požadovanou volbu. Chcete-li provést více než jednu úroveň kontroly ověření, spusťte úlohu monitoru pro každou úroveň, kterou potřebujete.

Je-li požadavek CICS DPL přečten monitorem mostu, spustí transakci zadanou v záhlaví CICS bridge (MQCIH), nebo pokud není zadána žádná transakce, transakce CKBP. ID uživatelů, pod kterými je spuštěný monitor mostu, musí mít oprávnění ke spuštění různých transakcí, které mohou být požadovány. Výchozí ID transakce pro monitor CICS bridge je CKBR, ale můžete změnit toto nebo definovat další ID transakcí, pokud chcete podrobnější přístup k frontám a transakcím. Můžete použít náhradní zabezpečení produktu CICS k omezení toho, které kombinace ID uživatele a transakce může spustit transakci monitoru mostu a ID uživatele.

Tabulka 64 na stránce 250 a Tabulka 65 na stránce 250 shrnují úroveň oprávnění pro monitor mostu a úlohy mostu a použití ID uživatele MQMD.

<i>Tabulka 64. Zabezpečení monitoru CICS bridge</i>		
<b>Monitor byl spuštěn uživatelem</b>	<b>Na přihlášené pokladně</b>	<b>Oprávnění monitoru</b>
Z terminálu nebo EXEC CICS LINK v rámci programu	Ano	Přihlášeno ID uživatele
Z terminálu nebo EXEC CICS LINK v rámci programu	Ne	CICS Předvolené ID uživatele
EXEC CICS START s ID uživatele	-	ID uživatele z relace START
EXEC CICS ZAČÁTEK bez ID uživatele	-	CICS Předvolené ID uživatele
Monitor spouštěčů IBM MQ CKTI	-	CICS Předvolené ID uživatele

<i>Tabulka 65. Zabezpečení úlohy produktu CICS bridge</i>	
<b>AUTH</b>	<b>Oprávnění k úlohám mostu</b>
LOKÁLNÍ	CICS Předvolené ID uživatele
IDENTIFIKOVAT	MQMD UserIdentifier
VERIFY_UOW	MQMD UserIdentifier
VERIFY_VŠE	MQMD UserIdentifier

Volby IDENTIFY, VERIFY\_UOW a VERIFY\_ALL vyžadují ID uživatele monitoru mostu definovaného pro produkt RACF jako náhrada všech ID uživatelů použitých ve zprávách požadavků. Tento požadavek je dodatkem k ID uživatele ve zprávě definované pro produkt RACF. (Náhradní uživatel je takový, který má oprávnění k zahájení práce jménem jiného uživatele, aniž by znal heslo jiného uživatele.)

Další informace o zabezpečení náhradního uživatele naleznete v příručce *CICS RACF Security Guide*.

**Poznámka:** Když se používá zabezpečení IDENTIFY, můžete vidět abend AICO pro CKBP, pokud se pokusíte spustit s ID uživatele, které bylo odvoláno. Chyba odpovědi má návratový kód MQCRC\_BRIDGE\_ERROR s příčinou MQFB\_CICS\_BRIDGE\_FAILURE.

*Oprávnění pro CICS bridge*

Komponenty mostu potřebují oprávnění k vložení nebo získání z různých front produktu IBM MQ .



V souhrnu je požadované oprávnění následující:

- Monitor a všechny úlohy mostu potřebují oprávnění k získání zpráv z fronty požadavků mostu.
- Úloha mostu potřebuje oprávnění k vkládání zpráv do své vlastní fronty pro odpověď.
- Aby bylo zajištěno, že jsou obdrženy jakékoli odpovědi na chyby, monitor potřebuje oprávnění k vkládání zpráv do všech front odpovědí.
- Úlohy mostu potřebují oprávnění k vkládání zpráv do fronty nedoručených zpráv.
- Monitor potřebuje oprávnění k umístění zpráv do fronty nedoručených zpráv, pokud nechcete, aby se most zastavil, dojde-li k chybě.
- Monitor a všechny úlohy mostu potřebují oprávnění k vkládání zpráv do fronty vrácených zpráv, je-li definována.

Chcete-li zjistit korelaci mezi ID uživatelů a oprávněním, prohlédněte si téma [Tabulka 64 na stránce 250](#).

## Aspekty zabezpečení pro použití produktu IBM MQ s produktem IMS

Toto téma popisuje, jak naplánovat požadavky na zabezpečení při použití produktu IBM MQ s produktem IMS.

### Použití třídy OPERCMDS

Pokud používáte produkt RACF k ochraně prostředků ve třídě OPERCMDS, ujistěte se, že ID uživatele přidružené k adresnímu prostoru správce front produktu IBM MQ má oprávnění k vydávání příkazu MODIFY pro libovolný systém IMS, ke kterému se může připojit.

### Aspekty zabezpečení pro most IMS

Existují čtyři aspekty, které musíte zvážit při rozhodování o svých požadavcích na zabezpečení mostu IMS :

- Jaká autorizace zabezpečení je zapotřebí pro připojení IBM MQ k IMS
- Kolik kontroly zabezpečení se provádí u aplikací, které používají most pro přístup k produktu IMS
- Které IMS prostředky jsou tyto aplikace povoleny pro použití
- Jaké oprávnění má být použito pro zprávy, které jsou vloženy do mostu a jsou k ní

Při definování požadavků zabezpečení pro most IMS je třeba vzít v úvahu následující skutečnosti:

- Zprávy procházející přes most mohly pocházet z aplikací na platformách, které nenabízejí silné ochranné prvky.
- Zprávy procházející přes most mohou pocházet z aplikací, které nejsou řízeny stejným podnikem nebo organizací.

### Aspekty zabezpečení pro připojení k produktu IMS

Udělte ID uživatele pro přístup k adresnímu prostoru správce front produktu IBM MQ přístup k skupině OTMA.

Most IMS je klientem OTMA. Připojení k produktu IMS pracuje pod ID uživatele adresního prostoru správce front produktu IBM MQ. Toto je obvykle definováno jako člen spuštěné skupiny úloh. Tomuto ID uživatele musí být udělen přístup ke skupině OTMA (není-li nastavení /SECURE OTMA nastaveno na hodnotu NONE).

Chcete-li to provést, definujte následující profil ve třídě FACILITY:

```
IMSXCF.xcfname.mqxcfname
```

Kde `xcfname` je název skupiny XCF a `mqxcfname` je název členu XCF produktu IBM MQ.

Do tohoto profilu je třeba udělit oprávnění pro čtení ID uživatele správce front produktu IBM MQ.

#### Poznámka:



1. Změníte-li oprávnění ve třídě FACILITY, musíte vydat příkaz RACF SETROPTS RACLIST (FACILITY) REFRESH, aby se změny aktivovaly.
2. Pokud profil hlq.NO.SUBSYS.SECURITY ve třídě MQADMIN existuje, není předáváno ID uživatele produktu IMS a připojení selže, pokud nastavení /SECURE OTMA není NONE.

### **Řízení přístupu k aplikacím pro most IMS**

Definujte profil RACF ve třídě FACILITY pro každý systém IMS . Udělte odpovídající úroveň přístupu k ID uživatele správce front produktu IBM MQ .

Pro každý systém IMS , ke kterému se most IMS připojuje, můžete definovat následující profil RACF ve třídě FACILITY, abyste určili, kolik kontroly zabezpečení se provádí pro každou zprávu předanou do systému IMS .

```
IMSXCF.xcfigname.imsxcfmname
```

Kde xcfigname je název skupiny XCF a imsxcfmname je název členu XCF pro IMS. (Pro každý systém IMS je třeba definovat samostatný profil.)

Úroveň přístupu, kterou povolíte pro ID uživatele správce front produktu IBM MQ v tomto profilu, je vrácena systému IBM MQ , pokud se most IMS připojuje k produktu IMSa označuje úroveň zabezpečení vyžadovanou při následných transakcích. V případě následných transakcí IBM MQ vyžádá příslušné služby z produktu RACF a, je-li ID uživatele autorizováno, předá zprávu do produktu IMS.

OTMA nepodporuje příkaz IMS /SIGN; produkt IBM MQ však umožňuje nastavit kontrolu přístupu pro každou zprávu, aby bylo možné povolit implementaci potřebné úrovně řízení.

Mohou být vráceny následující informace o úrovni přístupu:

#### **NEBYL NALEZEN**

Tyto hodnoty označují, že je vyžadováno maximální zabezpečení, tj. ověření je povinné pro každou transakci. Je provedena kontrola za účelem ověření, zda ID uživatele zadané v poli *UserIdentifier* struktury MQMD a heslo nebo PassTicket v poli *Ověřovatel* struktury MQIIH jsou známy produktu RACFa jsou platnou kombinací. UTOKEN se vytvoří s heslem nebo PassTicketa předá se do IMS ; UTOKEN se neukládá do mezipaměti.

**Poznámka:** Pokud profil hlq.NO.SUBSYS.SECURITY existuje ve třídě MQADMIN, tato úroveň zabezpečení přepíše všechny definice definované v profilu.

#### **READ (čtení)**

Tato hodnota indikuje, že má být provedeno stejné ověření jako pro NONE za následujících okolností:

- První, kdy je zjištěno určité ID uživatele
- Když bylo zjištěno ID uživatele před tím, než se položka UTOKEN uložená v mezipaměti nevytvořila pomocí hesla nebo PassTicket

Produkt IBM MQ vyžaduje v případě potřeby volbu UTOKEN a předává je produktu IMS.

**Poznámka:** Pokud byl vydán požadavek na opětovné ověření zabezpečení, jsou všechny informace uložené v mezipaměti ztraceny a UTOKEN je požadován při prvním výskytu každého ID uživatele.

#### **AKTUALIZOVAT**

Kontrola se provede, že ID uživatele v poli *UserIdentifier* struktury MQMD je známé jako RACF.

Společnost UTOKEN je sestavena a předána do produktu IMS ; UTOKEN se ukládá do mezipaměti.

#### **ŘÍZENÍ/ZMĚNA**

Tyto hodnoty indikují, že pro ID uživatelů tohoto systému IMS není třeba poskytnout žádné zabezpečení UTOKENs zabezpečení. (Tuto volbu byste pravděpodobně používali pouze pro vývojový a testovací systém.)



**Upozornění:** Všimněte si, že ID uživatele obsažené v poli *UserIdentifier* struktury MQMD je stále předáno pro **CONTROL/ALTER**.

### **Poznámka:**

1. Tento přístup je definován, když se produkt IBM MQ připojí k produktu IMSa trvá po dobu trvání připojení. Chcete-li změnit úroveň zabezpečení, je třeba změnit přístup k profilu zabezpečení a poté se přemostění zastavit a znovu spustit (například zastavením a restartováním OTMA).
2. Změníte-li oprávnění ve třídě FACILITY, musíte vydat příkaz RACF SETROPTS RACLIST (FACILITY) REFRESH, aby se změny aktivovaly.
3. Můžete použít heslo nebo PassTicket, ale musíte mít na paměti, že most IMS nešifruje data. Informace o použití PassTickets viz [“Použití RACF PassTickets v záhlaví IMS”](#) na stránce 254.
4. Některé z těchto výsledků mohou být ovlivněny nastavením zabezpečení v produktu IMS pomocí příkazu /SECURE OTMA.
5. Informace UTOKEN uložené v mezipaměti jsou drženy po dobu trvání definovanou parametry INTERVAL a TIMEOUT příkazu IBM MQ ALTER SECURITY.
6. Volba WARNING RACF nemá žádný vliv na profil IMSXCF.xcfgname.imsxcfmname . Jeho použití nemá vliv na úroveň uděleného přístupu a žádné zprávy RACF WARNING se nevytvorí.

### **Kontrola zabezpečení na systému IMS**

Zprávy, které procházejí přes most, obsahují informace o zabezpečení. Provedli se kontroly zabezpečení na základě nastavení příkazu IMS /SECURE OTMA.

Každá zpráva IBM MQ , která prochází přes most, obsahuje následující informace o zabezpečení:

- ID uživatele obsažené v poli *UserIdentifier* struktury MQMD.
- Obor zabezpečení obsažený v poli *SecurityScope* struktury MQIIH (je-li struktura MQIIH přítomná)
- Hodnota UTOKEN (pokud nemá podsystém IBM MQ přístup CONTROL nebo ALTER k příslušnému profilu IMSXCF.xcfgname.imsxcfmname )

Provedla se kontrola zabezpečení na nastavení příkazu IMS /SECURE OTMA, jak je uvedeno níže:

#### **/SECURE OTMA NONE**

Pro transakci nejsou provedeny žádné kontroly zabezpečení.

#### **/ZABEZPEČIT KONTROLU OTMMA**

Pole *UserIdentifier* struktury MQMD je předáno příkazu IMS pro kontrolu transakcí nebo kontroly příkazů.

Položka ACEE (Accessor Environment Element) je vestavěna v řídicí oblasti IMS .

#### **/SECURE OTMA FULL**

Pole *UserIdentifier* struktury MQMD je předáno příkazu IMS pro kontrolu transakcí nebo kontroly příkazů.

ACEE je postaven v IMS závislé oblasti a také v řídicí oblasti IMS .

#### **/SECURE OTMA PROFIL**

Pole *UserIdentifier* struktury MQMD je předáno příkazu IMS pro kontrolu transakcí nebo oprávnění k příkazům.

Pole *SecurityScope* ve struktuře MQIIH se používá k určení, zda má být v IMS závislé oblasti a oblasti ovládacího prvku sestavované ACEE sestavované.

### **Poznámka:**

1. Pokud změníte oprávnění ve třídě TIMS nebo CIMS nebo přidružené třídy skupin GIMS nebo DIMS, musíte pro aktivaci změn vydat následující příkazy IMS :
  - /MODIFY PREPARE RACF
  - /UPRAVIT POTVRZENÍ
2. Pokud nepoužíváte /SECURE OTMA PROFILE, bude ignorována libovolná hodnota uvedená v poli *SecurityScope* struktury MQIIH.

## **Kontrola zabezpečení provedená pomocí mostu IMS**

Různí oprávnění se používají v závislosti na prováděné akci.

Když most vloží nebo získá zprávu, použijí se následující oprávnění:

### **Získání zprávy z fronty mostu**

Neprovedou se žádné kontroly zabezpečení.

### **Vložení výjimky nebo zprávy sestavy COA**

Používá oprávnění ID uživatele v poli *UserIdentifier* struktury MQMD.

### **Vložení zprávy s odpovědí**

Používá oprávnění ID uživatele v poli *UserIdentifier* struktury MQMD v původní zprávě.

### **Vložení zprávy do fronty nedoručených zpráv**

Neprovedou se žádné kontroly zabezpečení.

### **Poznámka:**

1. Změníte-li profily tříd produktu IBM MQ , je třeba provést aktivaci změn zadáním příkazu IBM MQ REFRESH SECURITY (\*).
2. Pokud změníte oprávnění uživatele, musíte pro aktivaci této změny vydat příkaz MQSC RVERIFY SECURITY.

## **Použití RACF PassTickets v záhlaví IMS**

PassTicket můžete použít místo hesla v záhlaví IMS .

Pokud chcete použít PassTicket místo hesla v záhlaví IMS (MQIIH), uveďte jméno aplikace, proti které je PassTicket validován v atributu PASSTKTA definice STGCLASS fronty mostu IMS , do které má být zpráva směřována.

Je-li hodnota PASSTKTA ponechána prázdná, musíte zařídit, aby byl vygenerován PassTicket . Název aplikace v tomto případě musí být ve formátu MVSxxxx, kde xxxx je SMFID systému z/OS , na kterém je spuštěn cílový správce front.

PassTicket je sestaven z ID uživatele, cílového názvu aplikace a tajného klíče. Jedná se o 8bajtovou hodnotu obsahující velká písmena a číslice. Lze jej použít pouze jednou a je platný po dobu 20 minut. Pokud je PassTicket generován lokálním systémem RACF , RACF pouze kontroluje, zda profil existuje a ne, že má uživatel oprávnění k tomuto profilu. Pokud byl PassTicket generován na vzdáleném systému, produkt RACF ověří přístup ID uživatele k profilu. Informace o úplných informacích o PassTickets viz příručka *z/OS SecureWay Security Server RACF Security Administrator's Guide*.

PassTickets v záhlaví IMS se dává RACF do IBM MQ, ne IMS.

## **Nastavení zabezpečení produktu IBM MQ MQI client**

Je třeba zvážit zabezpečení produktu IBM MQ MQI client , aby klientské aplikace neměly neomezený přístup k prostředkům na serveru.

Když spouštíte aplikaci klienta, nespouštějte aplikaci pomocí ID uživatele, které má více přístupových práv, než je nezbytné, například uživatel ve skupině mqm nebo dokonce sám uživatel mqm .

Spustíte-li aplikaci jako uživatele s příliš mnoha přístupovými právy, riskujete přístup k aplikaci a změnou částí správce front, a to buď omylem, nebo neúmyslně.

Mezi aplikací klienta a jeho serverem správce front existují dva aspekty zabezpečení: ověřování a řízení přístupu.

- Ověřování lze použít k ujištění, že klientská aplikace spuštěná jako specifický uživatel je tím, kým říkají, že jsou. Použitím ověření můžete zabránit útočníkovi získat přístup k vašemu správci front tím, že zosobňujete jednu z vašich aplikací.

V produktu IBM MQ 8.0 je ověření poskytnuto jednou ze dvou možností:

- Funkce ověření připojení.

Další informace o ověření připojení viz [“Ověření připojení”](#) na stránce 55.

- Použití vzájemného ověření v rámci SSL nebo TLS.

Další informace o SSL nebo TLS najdete v tématu [“Práce s SSL nebo TLS”](#) na stránce 259.

- 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 333.

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 364.

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 48.

## **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 MQCONN 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 MQCONN poskytnout novou hodnotu pro FipsRequired.

Je-li přítomen kryptografický hardware, mohou být kryptografické moduly používané produktem IBM 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 IBM MQ nezaručuje odmítnutí všech takových připojení a je vaší odpovědností určit, zda je vaše konfigurace produktu IBM MQ kompatibilní se standardem FIPS-.

### **Související pojmy**

[“Federální standardy zpracování informací \(FIPS\) pro SYSTÉM UNIX, Linuxa Okna”](#) na stránce 32

When cryptography is required on an SSL/TLS channel on Windows, SYSTÉM UNIX a Linux systems, IBM MQ uses a cryptography package called IBM Crypto for C (ICC). Na platformách Windows, SYSTÉM UNIX a Linux , schválil software ICC standardy FIPS (Federal Information Processing Standards) programu US National Institute of Standards and Technology (Federal Information Processing Standards) na úrovni 140-2.

### Související informace

[FipsRequired \(MQLONG\)](#)

[MQSSLFIPS](#)

[stanza SSL konfiguračního souboru klienta](#)

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

Klientské aplikace SSL nebo TLS v produktu AIX mohou zaznamenat MQRC\_CHANNEL\_CONFIG\_ERROR a chybu AMQ6175 , pokud jsou spuštěny na systémech AIX s více instalacemi sady GSKit V8.0 .

Při spouštění klientských aplikací na systému AIX s více instalacemi sady GSKit V8.0 může volání spojení klienta vrátit produkt MQRC\_CHANNEL\_CONFIG\_ERROR při použití zabezpečení 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_9GSKASN0ID (number 16) is not
exported from dependent module /db2data/db2inst1/sqllib/lib64/libgsk8cms_64.so.
  Symbol VALUE_EC_NamedCurve_secp384r1_9GSKASN0ID (number 17) is not exported from
dependent module /db2data/db2inst1/sqllib/lib64/libgsk8cms_64.so.
  Symbol VALUE_EC_NamedCurve_secp521r1_9GSKASN0ID (number 18) is not exported from
dependent module /db2data/db2inst1/sqllib/lib64/libgsk8cms_64.so.
  Symbol VALUE_EC_ecPublicKey_9GSKASN0ID (number 19) is not exported from dependent
module /db2data/db2inst1/sqllib/lib64/libgsk8cms_64.so.
  Symbol VALUE_EC_ecdsa_with_SHA1_9GSKASN0ID (number 20) is not exported from
dependent module /db2data/db2inst1/sqllib/lib64/libgsk8cms_64.so.
  Symbol VALUE_EC_ecdsa_9GSKASN0ID (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.

```
----- amqcgkska.c : 836 -----
```

Běžnou příčinou této chyby je to, že nastavení proměnné prostředí LIBPATH nebo LD\_LIBRARY\_PATH způsobilo, že klient produktu IBM MQ zaváděl smíšenou sadu knihoven ze dvou různých instalací sady GSKit V8.0 . Tato chyba může způsobit provedení klientské aplikace IBM MQ v prostředí produktu Db2 .

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

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

Další informace o použití příkazu **setmqenv** naleznete v části [setmqenv \(nastavení prostředí IBM MQ\)](#)

## IBM i **Nastavení komunikace pro SSL nebo TLS v systému IBM i**

Zabezpečené komunikace, které používají šifrovací bezpečnostní protokoly SSL nebo TLS, zahrnují nastavení komunikačních kanálů a správu digitálních certifikátů, které budete používat pro ověření.

Chcete-li nastavit zabezpečení SSL nebo TLS, je třeba definovat kanály pro použití zabezpečení SSL nebo TLS. Musíte také vytvořit a spravovat digitální certifikáty. V některých operačních systémech můžete provádět testy s certifikáty s vlastním podpisem. V systému IBM i však musíte používat osobní certifikáty podepsané lokálním CA.

Chcete-li získat úplné informace o vytváření a správě certifikátů, prohlédněte si téma [“Práce s SSL nebo TLS v systému IBM i”](#) na stránce 262.

Tato kolekce témat představuje některé z úloh souvisejících s nastavením komunikace SSL nebo TLS a poskytuje pokyny k provedení těchto úloh podle kroku.

Možná budete chtít testovat také ověření klienta SSL nebo TLS, které jsou volitelné části protokolů SSL a TLS. Při navázání komunikace přes zabezpečení SSL nebo TLS vždy klient SSL nebo TLS získává a ověřuje digitální certifikát ze serveru. Při použití implementace produktu IBM MQ server SSL nebo TLS vždy požaduje certifikát od klienta.

V systému IBM i odešle klient SSL nebo TLS certifikát pouze v případě, že má jeden označený ve správném formátu IBM MQ :

- V případě správce front se hodnota `ibmwebspheremq` následovaná názvem správce front změnila na malá písmena. Například pro QM1, `ibmwebspheremqm1`.
- Pro klienta IBM MQ C for IBM i, `ibmwebspheremq` následovalo vaše přihlašovací ID uživatele se změnil na malá písmena, například `ibmwebspheremqmyuserid`.

IBM MQ používá předponu `ibmwebspheremq` na štítku, aby nedošlo k záměně s certifikáty pro jiné produkty. Ujistěte se, že jste zadali celé návštěvní certifikátu malými písmeny.

Server SSL nebo TLS vždy ověřuje platnost certifikátu klienta, je-li odeslán. Pokud klient SSL nebo TLS neodešle certifikát, ověření selže pouze tehdy, když je konec kanálu, který funguje jako server SSL nebo TLS, definován buď s parametrem `SSLCAUTH` nastaveným na hodnotu `REQUIRED` nebo nastaveným na hodnotu parametru `SSLPEER`. Další informace naleznete v tématu [Připojení dvou správců front s použitím zabezpečení SSL nebo TLS](#).

## **distributed** **Nastavení komunikace pro zabezpečení SSL nebo TLS v systémech UNIX, Linux nebo 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.



**Upozornění:** Není možné použít směs certifikátů podepsaných Elliptic Curve a RSA podepsaných pro správce front, které chcete spojit pomocí kanálů s povoleným zabezpečením TLS.

Správci front používající kanály s povoleným zabezpečením TLS musí všechny používat certifikáty podepsané RSA nebo všechny certifikáty podepsané EC, nikoli směs obou těchto certifikátů.

Další informace viz [“Digitální certifikáty a kompatibilita CipherSpec v produktu IBM MQ”](#) na stránce 44.



Certifikáty podepsané sebou samým nelze odvolat, což by mohlo útočnickovi 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 v systémech UNIX, Linux a Windows”](#) na stránce 273.

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 TLS, které je volitelnou částí protokolů. Při navázání komunikace přes zabezpečení SSL nebo TLS vždy klient SSL nebo TLS získává a ověřuje digitální certifikát ze serveru. Při použití implementace produktu IBM MQ server SSL nebo TLS vždy požaduje certifikát od klienta.

V systémech UNIX, Linux a Windows odešle klient SSL nebo TLS certifikát pouze v případě, že má jeden označený ve správném formátu IBM MQ :

- V případě správce front je formát `ibmwebspheremq` následován názvem správce front, který byl změněn na malá písmena. Například pro QM1, `ibmwebspheremqm1`
- V případě klienta IBM MQ je `ibmwebspheremq` následováno vaším přihlašovacím ID uživatele změněno na malá písmena, například `ibmwebspheremqmyuserid`.

IBM MQ používá předponu `ibmwebspheremq` na štítku, aby nedošlo k záměně s certifikáty pro jiné produkty. Ujistěte se, že jste zadali celé návěští certifikátu malými písmeny.

Server SSL nebo TLS vždy ověřuje platnost certifikátu klienta, je-li odeslán. Pokud klient neodešle certifikát, ověření selže pouze tehdy, když je konec kanálu, který funguje jako server SSL nebo TLS, definován buď s parametrem `SSLCAUTH` nastaveným na hodnotu `REQUIRED` nebo s nastavenou hodnotou parametru `SSLPEER`. Další informace naleznete v tématu [Připojení dvou správců front s použitím zabezpečení SSL nebo TLS](#).

**z/OS**

## Nastavení komunikace pro SSL nebo TLS v systému z/OS

Zabezpečené komunikace, které používají šifrovací bezpečnostní protokoly SSL nebo TLS, zahrnují nastavení komunikačních kanálů a správu digitálních certifikátů, které budete používat pro ověření.

Chcete-li nastavit zabezpečení SSL nebo TLS, je třeba definovat kanály pro použití zabezpečení SSL nebo TLS. Musíte také vytvořit a spravovat digitální certifikáty. V systému z/OS můžete provádět testy s certifikáty s vlastním podpisem nebo s osobními certifikáty podepsanými lokálním vydavatelem certifikátů (CA).

Certifikáty podepsané sebou samým nelze odvolat, což by mohlo útočnickovi umožnit, aby se identita po soukromém klíči zkompromitovala. Certifikační úřady mohou odvolat kompromitovaný certifikát, který zabrání jeho dalšímu použití. Certifikáty podepsané certifikační autoritou jsou proto bezpečnější pro použití v produkčním prostředí, ačkoli certifikáty podepsané sebou samým pro testovací systém jsou pohodlnější.

Chcete-li získat úplné informace o vytváření a správě certifikátů, prohlédněte si téma [“Práce s SSL nebo TLS v systému z/OS”](#) na stránce 304.

Tato kolekce témat představuje některé z úloh souvisejících s nastavením komunikace SSL nebo TLS a poskytuje pokyny pro dokončení těchto úloh krok za krokem.

Možná budete chtít testovat také ověření klienta SSL nebo TLS, které jsou volitelnou částí protokolů. Při navázání komunikace přes zabezpečení SSL nebo TLS vždy klient SSL nebo TLS získává a ověřuje digitální certifikát ze serveru. Při použití implementace produktu IBM MQ server SSL nebo TLS vždy požaduje certifikát od klienta.

V systému z/OS klient SSL nebo TLS odešle certifikát pouze v případě, že má jeden z následujících certifikátů:

- Pouze pro sdílený kanál, certifikát se jmenovkou ve formátu `ibmWebSphereMQ` následovaný názvem skupiny sdílení front, například `ibmWebSphereMQQSG1`
- Certifikát se jmenovkou ve formátu `ibmWebSphereMQ` následovaný názvem vašeho správce front, například `ibmWebSphereMQQM1`
- Výchozí certifikát (který může být certifikátem `ibmWebSphereMQ`).

Je-li kanál sdílený, kanál se nejprve pokusí najít certifikát pro skupinu sdílení front. Pokud se nenajde certifikát pro skupinu sdílení front, pokusí se najít certifikát pro správce front.

V systému z/OS používá produkt IBM MQ předponu `ibmWebSphereMQ` na štítku, aby nedošlo k záměně s certifikáty pro jiné produkty.

Server SSL nebo TLS vždy ověřuje platnost certifikátu klienta, je-li odeslán. Pokud klient SSL nebo TLS neodešle certifikát, ověření selže pouze tehdy, když je konec kanálu, který funguje jako server SSL nebo TLS, definován buď s parametrem `SSLCAUTH` nastaveným na hodnotu `REQUIRED` nebo nastaveným na hodnotu parametru `SSLPEER`. Další informace naleznete v tématu [Připojení dvou správců front s použitím zabezpečení SSL nebo TLS](#).

## Práce s SSL nebo TLS

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

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

- [“Identifikace a ověřování uživatelů”](#) na stránce 315
- [“Autorizace přístupu k objektům”](#) na stránce 333
- [“Důvěrnost zpráv”](#) na stránce 392
- [“Integrita dat zpráv”](#) na stránce 403
- [“Uchování zabezpečených klastrů”](#) na stránce 404

## Práce s SSL nebo TLS v systému HP Integrity NonStop Server

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

Podpora zabezpečení SSL & TLS produktu IBM 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 MQ pro produkt HP Integrity NonStop Server se skládá z následujících komponent:

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

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

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

## Podporované verze protokolu

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

- SSL 3.0
- TLS 1.0



- TLS 1.2

### **Podporované CipherSpecs**

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

- “Úložiště osobních certifikátů” na stránce 261
- “Certifikát o důvěryhodnosti” na stránce 261
- “Předat soubor pro uložení fráze” na stránce 261
- “Soubor se seznamem odvolaných certifikátů” na stránce 262

#### *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 vlastnímu úložišti 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 frázi schválení Stash.sth.

#### *Certifikát o důvěryhodnosti*

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 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 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 vlastnímu přidruženému úložišti 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 s SSL nebo TLS v systému IBM i

Tato kolekce témat obsahuje pokyny pro jednotlivé úlohy, které pracují se zabezpečením SSL (Secure Sockets Layer) nebo TLS (Transport Layer Security) v produktu IBM MQ for IBM i.

Pro IBM i je podpora SSL integrální součástí operačního systému. Ujistěte se, že jste nainstalovali nezbytné předpoklady uvedené v tématu [Hardwarové a softwarové požadavky na produktu IBM i](#).

V systému IBM ispravujete klíče a digitální certifikáty pomocí nástroje Digital Certificate Manager (DCM).

### ***Přístup k DCM***

Postupujte podle těchto pokynů pro přístup k rozhraní DCM.

### **Informace o této úloze**

Proveďte následující kroky ve webovém prohlížeči, který podporuje rámce.

### **Postup**

1. Přejděte do adresáře `http://machine.domain:2001` nebo `https://machine.domain:2010`, kde *machine* je název vašeho počítače.
2. Zadejte platný uživatelský profil a heslo, je-li to požadováno.  
Ujistěte se, že váš uživatelský profil má speciální oprávnění `*ALLOBJ` a `*SECADM`, abyste mohli vytvářet nová úložiště certifikátů. Nemáte-li speciální oprávnění, můžete spravovat pouze své osobní certifikáty nebo zobrazit podpisy objektů pro objekty, pro které máte oprávnění. Máte-li oprávnění k použití aplikace pro podepisování objektů, můžete také podepisovat objekty z DCM.
3. Na stránce Konfigurace Internetu klepněte na **Digital Certificate Manager**.

Zobrazí se stránka Digitální Certificate Manager .

### **Přiřazení certifikátu ke správci front v systému IBM i**

Použijte produkt DCM k přiřazení certifikátu ke správci front.

K přiřazení certifikátu ke správci front použijte tradiční správu digitálních certifikátů produktu IBM i . To znamená, že můžete uvést, že správce front používá systémové úložiště certifikátů a že je správce front registrován pro použití jako aplikace s DCM (Digital Certificate Manager. Chcete-li to provést, změňte hodnotu atributu **SSLKEYR** správce front na \*SYSTEM.

Je-li parametr **SSLKEYR** změněn na \*SYSTEM, produkt IBM MQ registruje správce front jako serverovou aplikaci s jedinečným popisem aplikace fronty QIBM\_WEBSPPHERE\_MQ\_QMGRNAME a štítkem s popisem Qmgrname (WMQ). Všimněte si, že atributy kanálu **CERTLABL** se nepoužijí, používáte-li paměť certifikátů \*SYSTEM. Správce front se poté zobrazí jako serverová aplikace v produktu Digital Certificate Managera můžete této aplikaci přiřadit libovolný serverový nebo klientský certifikát v systémovém úložišti.

Vzhledem k tomu, že správce front je registrován jako aplikace, lze provádět rozšířené funkce produktu DCM, jako je například definování důvěryhodných seznamů CA.

Pokud se parametr **SSLKEYR** změní na jinou hodnotu než \*SYSTEM, IBM MQ zruší registraci správce front jako aplikaci s DCM (Digital Certificate Manager. Je-li správce front odstraněn, je také z DCM deregistrován. Uživatel s dostatečným oprávněním \*SECADM může také ručně přidávat nebo odebírat aplikace z DCM.

### **Nastavení úložiště klíčů v systému IBM i**

Na obou koncích připojení musí být nastaveno úložiště klíčů. Lze použít výchozí úložiště certifikátů, nebo můžete vytvořit vlastní úložiště certifikátů.

Připojení SSL nebo TLS vyžaduje *úložiště klíčů* na každém konci připojení. Každý správce front a produkt IBM MQ MQI client musí mít přístup k úložišti klíčů. Chcete-li přistoupit k úložišti klíčů pomocí názvu souboru a hesla (tj. ne pomocí volby \*SYSTEM), ujistěte se, že uživatelský profil QMQM má následující oprávnění:

- Oprávnění k provedení pro adresář obsahující úložiště klíčů
- Oprávnění ke čtení pro soubor obsahující úložiště klíčů

Další informace viz [“Úložiště klíčů SSL nebo TLS”](#) na stránce 23. Všimněte si, že atributy kanálu **CERTLABL** se nepoužijí, používáte-li paměť certifikátů \*SYSTEM.

V systému IBM i jsou digitální certifikáty uloženy v úložišti certifikátů, které je spravováno produktem DCM. Tyto digitální certifikáty mají štítky, které přidružují certifikát ke správci front nebo k produktu IBM MQ MQI client. SSL a TLS používají certifikáty pro účely autentizace.

Jmenovka je buď hodnota atributu **CERTLABL** , je-li nastavena, nebo standardní `ibmwebspheremq` s připojeným jménem správce front nebo přihlašovacího ID uživatele IBM MQ MQI client , vše malými písmeny. Podrobnosti najdete v tématu [Digitální certifikáty certifikátu](#) .

Název správce front nebo úložiště certifikátů produktu IBM MQ MQI client se skládá z cesty a názvu kmene. Výchozí cesta je `/QIBM/UserData/ICSS/Cert/Server/` a výchozí název kmene je `Default`. V produktu IBM i je výchozí úložiště certifikátů, `/QIBM/UserData/ICSS/Cert/Server/Default.kdb`, také známé jako \*SYSTEM. Volitelně můžete definovat vlastní cestu a název kmene.

Definujete-li vlastní cestu nebo název souboru, nastavte oprávnění k souboru tak, aby k němu měl přístup těsně pod kontrolou.

Příkaz [“Změna umístění úložiště klíčů pro správce front v systému IBM i”](#) na stránce 265 vám sděluje informace o určení názvu úložiště certifikátů. Název úložiště certifikátů můžete zadat buď před vytvořením úložiště certifikátů, nebo po něm.

**Poznámka:** Operace, které můžete provádět s DCM, mohou být omezeny oprávněním vašeho uživatelského profilu. Například vyžadujete oprávnění \*ALLOBJ a \*SECADM pro vytvoření certifikátu CA.

## Vytvoření úložiště certifikátů v systému IBM i

Pokud nechcete použít výchozí úložiště certifikátů, postupujte podle této procedury a vytvořte vlastní úložiště certifikátů.

### Informace o této úloze

Vytvořte nové úložiště certifikátů pouze v případě, že nechcete používat výchozí úložiště certifikátů produktu IBM i .

Chcete-li určit, že má být použito úložiště certifikátů systému IBM i , změňte hodnotu atributu SSLKEYR správce front na \*SYSTEM. Tato hodnota označuje, že správce front používá systémové úložiště certifikátů a správce front je registrován pro použití jako aplikace s produktem DCM (Digital Certificate Manager).

### Postup

1. Přejděte k rozhraní DCM, jak je popsáno v [“Přístup k DCM”](#) na stránce 262
2. V navigačním panelu klepněte na volbu **Vytvořit nové úložiště certifikátů**.  
V rámci úlohy se zobrazí stránka Vytvoření nové paměti certifikátů.
3. V rámci úlohy vyberte volbu **Jiná systémová paměť certifikátů** a klepněte na tlačítko **Pokračovat**.  
V rámci úlohy se zobrazí stránka Vytvoření certifikátu v nové paměti certifikátů.
4. Vyberte volbu **Ne-Nevytvářet certifikát v úložišti certifikátů** a klepněte na tlačítko **Pokračovat**.  
V rámci úlohy se zobrazí stránka Název úložiště certifikátů a heslo.
5. Do pole **Cesta k úložišti certifikátů a název souboru** zadejte cestu k souboru IFS a název souboru, například /QIBM/UserData/mqm/qmgrs/qm1/key.kdb
6. Do pole **Heslo** zadejte heslo a zadejte je znovu do pole **Potvrdit heslo** . Klepněte na tlačítko **Pokračovat**.  
Poznamenejte si heslo (je citlivé na velikost písmen), protože jej budete potřebovat při ukládání klíče úložiště.
7. Chcete-li ukončit práci s produktem DCM, zavřete okno prohlížeče.

### Jak pokračovat dále

Když jste vytvořili paměť certifikátů pomocí produktu DCM, ujistěte se, že jste heslo uložili, jak je popsáno v [“Uložení hesla k úložišti certifikátů v systémech IBM i”](#) na stránce 264

#### Související úlohy

[“Import certifikátu do úložiště klíčů v systému IBM i”](#) na stránce 269

Chcete-li importovat certifikát, postupujte podle této procedury.

#### *Uložení hesla k úložišti certifikátů v systémech IBM i*

Založit heslo k úložišti certifikátů pomocí CL příkazů.

Následující pokyny se vztahují na ukládání hesla úložiště certifikátů v systému IBM i pro správce front. Alternatively, for an IBM MQ MQI client, if you are not using the \*SYSTEM certificate store (that is, the MQSSLKEYR environment is set to a value other than \*SYSTEM), follow the procedure described in the [“Ukládání hesla k úložišti certifikátů”](#) na stránce 272 section of [“Obslužný program IBM MQ SSL Client \(amqrssl\) pro IBM i”](#) na stránce 271.

Jestliže jste uvedli, že paměť certifikátů \*SYSTEM má být použita (změnou hodnoty atributu SSLKEYR ze správce front na \*SYSTEM), nesmíte tyto kroky provést.

Když jste pomocí produktu DCM vytvořili úložiště certifikátů, použijte následující příkazy k uložení hesla:

```
STRMQM MQMNAME('queue manager name')
CHGMQM MQMNAME('queue manager name') SSLKEYRPWD('password')
```

Heslo, které rozlišuje velikost písmen, musí být uvedeno v jednoduchých uvozovkách přesně tak, jak jste je zadali v kroku 6 dokumentu [“Vytvoření úložiště certifikátů v systému IBM i”](#) na stránce 264.

**Poznámka:** Pokud nepoužíváte výchozí systémové úložiště certifikátů a neuložíte heslo, pokusy o spuštění kanálů SSL se nezdaří, protože nemohou získat heslo potřebné pro přístup k paměti certifikátů.

## ***Vyhledání úložiště klíčů pro správce front v systému IBM i***

Tento postup slouží k získání umístění úložiště certifikátů správce front.

### **Postup**

1. Zobrazte atributy správce front pomocí následujícího příkazu:

```
DSPMQM MQMNAME('queue manager name')
```

2. Provéřte výstup příkazu pro cestu a název kmene úložiště certifikátů.

Například: /QIBM/UserData/ICSS/Cert/Server/Default, kde /QIBM/UserData/ICSS/Cert/Server je cesta a Default je název kmene.

## ***Změna umístění úložiště klíčů pro správce front v systému IBM i***

Změňte umístění úložiště certifikátů správce front pomocí příkazu CHGMQM nebo ALTER QMGR.

### **Postup**

Pro nastavení atributu úložiště klíčů správce front použijte buď příkaz CHGMQM, nebo příkaz ALTER QMGR MQSC.

- a) Použití CHGMQM: CHGMQM MQMNAME('qm1') SSLKEYR('/QIBM/UserData/ICSS/Cert/Server/MyKey')
- b) Použití příkazu ALTER QMGR: ALTER QMGR SSLKEYR('/QIBM/UserData/ICSS/Cert/Server/MyKey')

V obou případech má úložiště certifikátů plně kvalifikovaný název souboru: /QIBM/UserData/ICSS/Cert/Server/MyKey.kdb

### **Jak pokračovat dále**

Změníte-li umístění úložiště certifikátů správce front, nebudou certifikáty přeneseny ze starého umístění. Pokud jsou certifikáty CA předinstalované při vytváření úložiště certifikátů nedostatečné, je třeba naplnit nové úložiště certifikátů certifikáty, jak je popsáno v tématu [“Import certifikátu do úložiště klíčů v systému IBM i”](#) na stránce 269. Musíte také odložit heslo pro nové umístění, jak je popsáno v tématu [“Uložení hesla k úložišti certifikátů v systémech IBM i”](#) na stránce 264.

## ***Vytvoření certifikační autority a certifikátu pro testování v systému IBM i***

Tento postup slouží k vytvoření certifikátu lokálního CA pro podepisování požadavků na certifikát a k vytvoření a instalaci certifikátu CA.

### **Než začnete**

Pokyny v tomto tématu předpokládají, že lokální certifikační autorita (CA) neexistuje. Pokud lokální CA existuje, přejděte na [“Požadání o certifikát serveru v systému IBM i”](#) na stránce 266.

### **Informace o této úloze**

Certifikáty CA, které jsou poskytovány při instalaci zabezpečení SSL, jsou podepsány vydavatelem CA. V systému IBM i můžete generovat lokální certifikační autoritu, která může podepisovat certifikáty serveru pro účely testování komunikace SSL ve vašem systému. Chcete-li vytvořit lokální certifikát CA, postupujte takto ve webovém prohlížeči:

### **Postup**

1. Přistupte k rozhraní DCM, jak je popsáno v tématu [“Přístup k DCM”](#) na stránce 262.
2. V navigačním panelu klepněte na volbu **Vytvořit certifikační autoritu**.

- V rámci úlohy se zobrazí stránka Vytvoření certifikační autority.
3. Do pole **Heslo úložiště certifikátů** zadejte heslo a zadejte jej znovu do pole **Potvrdit heslo** .
  4. Zadejte název do pole **Název vydavatele certifikátů (CA)** , například SSL Test Certificate Authority.
  5. Zadejte příslušné hodnoty do polí **Obecný název** a **Organizace** a vyberte zemi. Pro zbývající volitelná pole zadejte požadované hodnoty.
  6. Do pole **Období platnosti** zadejte období platnosti pro lokálního CA.  
Výchozí hodnota je 1095 dnů.
  7. Klepněte na tlačítko **Pokračovat**.  
Vytvoří se CA a DCM vytvoří paměť certifikátů a certifikát CA pro vašeho lokálního CA.
  8. Klepněte na tlačítko **Instalovat certifikát**.  
Zobrazí se dialogové okno správce stahování.
  9. Zadejte úplnou cestu k dočasnému souboru, do kterého chcete uložit certifikát CA, a klepněte na tlačítko **Uložit**.
  10. Jakmile je stahování dokončeno, klepněte na tlačítko **Otevřít**.  
Zobrazí se okno certifikátu.
  11. Klepněte na tlačítko **Instalovat certifikát**.  
Zobrazí se průvodce importem certifikátu.
  12. Klepněte na tlačítko **Další**.
  13. Vyberte volbu **Automaticky vybrat paměť certifikátů na základě typu certifikátu** a klepněte na tlačítko **Další**.
  14. Klepněte na tlačítko **Dokončit**.  
Zobrazí se potvrzovací okno.
  15. Klepněte na tlačítko **OK**.
  16. V okně Certifikát klepněte na tlačítko **OK**.
  17. Klepněte na tlačítko **Pokračovat**.  
Stránka Zásada certifikační autority se zobrazí v rámci úlohy.
  18. V poli **Povolit vytvoření uživatelských certifikátů** vyberte volbu **Ano**.
  19. Do pole **Období platnosti** zadejte období platnosti certifikátů, které jsou vydány vašim lokálním CA.  
Výchozí hodnota je 365 dní.
  20. Klepněte na tlačítko **Pokračovat**.  
V rámci úlohy se zobrazí stránka Vytvoření certifikátu v nové paměti certifikátů.
  21. Zkontrolujte, zda není vybrána žádná z aplikací.
  22. Chcete-li dokončit nastavení lokálního CA, klepněte na **Pokračovat** .

### **Požádání o certifikát serveru v systému IBM i**

Digitální certifikáty chrání před ztělesněním a potvrzují, že veřejný klíč patří do zadané entity. Certifikát nového serveru lze požadovat od vydavatele certifikátů pomocí produktu DCM (Digital Certificate Manager).

### **Informace o této úloze**

Ve webovém prohlížeči proveďte následující kroky:

### **Postup**

1. Přistupte k rozhraní DCM, jak je popsáno v tématu [“Přístup k DCM”](#) na stránce 262.
2. V navigačním panelu klepněte na **Výběr úložiště certifikátů**.  
V rámci úlohy se zobrazí stránka Výběr úložiště certifikátů.
3. Vyberte úložiště certifikátů, které chcete použít, a klepněte na **Pokračovat**.



4. Volitelné: Pokud jste v kroku 3 vybrali **\*SYSTEM** , zadejte heslo do systémového úložiště a klepněte na **Pokračovat**.
5. Volitelné: Pokud jste v kroku 3 vybrali volbu **Jiná systémová paměť certifikátů** , v poli **Cesta k úložišti certifikátů a název souboru** zadejte cestu k souboru IFS a název souboru, který jste nastavili při vytváření paměti certifikátů. Do pole **Heslo úložiště certifikátů** zadejte také heslo. Pak klepněte na **Pokračovat**
6. V navigačním panelu klepněte na volbu **Vytvořit certifikát**.
7. V rámci úlohy vyberte přepínač **Certifikát serveru nebo klienta** a klepněte na tlačítko **Pokračovat**.  
V rámci úlohy se zobrazí stránka Select a Certificate Authority (CA).
8. Máte-li na pracovní stanici lokálního CA, zvolte buď lokální CA, nebo komerční CA k podepsání certifikátu. Vyberte přepínač pro CA, který chcete, a klepněte na **Pokračovat**.  
V rámci úlohy se zobrazí stránka Vytvoření certifikátu.
9. Volitelné: V případě správce front zadejte do pole **Popisek certifikátu** jmenovku certifikátu.  
Jmenovka je buď hodnota atributu **CERTLABL** , pokud je nastavena, nebo standardní `ibmwebspheremq` s připojeným názvem správce front, vše malými písmeny. Podrobnosti najdete v tématu [Digitální certifikáty certifikátu](#) .  
Například pro správce front QM1zadejte `ibmwebspheremqqm1` pro použití výchozí hodnoty.
10. Volitelné: Pro IBM MQ MQI clientv poli **Označení certifikátu** zadejte `ibmwebspheremq` následované ID uživatele pro přihlášení složené na malá písmena.  
Zadejte například `ibmwebspheremqmyuserid`
11. Zadejte příslušné hodnoty do polí **Obecný název** a **Organizace** a vyberte zemi. Pro zbývající volitelná pole zadejte požadované hodnoty.

## Výsledky

Pokud jste vybrali komerční CA k podepsání vašeho certifikátu, produkt DCM vytvoří žádost o certifikát ve formátu PEM (Privacy-Enhanced Mail). Postoupit požadavek na zvolenou CA.

Pokud jste vybrali lokálního CA pro podepsání vašeho certifikátu, produkt DCM vás informuje o tom, že certifikát byl vytvořen v paměti certifikátů a lze jej použít.

## Vyžádání certifikátu serveru v produktu IBM i for IBM Key Manager

Postupujte takto, chcete-li vytvořit certifikát podepsaný vaší lokální certifikační autoritou (CA) nebo požádat o certifikát serveru podepsaný komerční CA pro import do obslužného programu iKeyman (Správa klíčů produktu IBM).

## Informace o této úloze

Certifikát uživatele musí být použit, když DCM (Digital Certificate Manager) slouží jako správce certifikátů pro IBM MQ na více platformách. V případě osobních certifikátů distribuovaných na jiných platformách a pro import do obslužného programu iKeyman proveďte ve webovém prohlížeči následující kroky:

## Postup

1. Přistupte k rozhraní DCM, jak je popsáno v tématu [“Přístup k DCM”](#) na stránce 262.
2. V podokně **navigace** klepněte na volbu **Vytvořit certifikát**.  
Stránka **Vytvořit certifikát** se zobrazí v rámci úlohy.
3. Na panelu **Vytvořit certifikát** vyberte přepínač **Certifikát uživatele** a klepněte na tlačítko **Pokračovat**.  
Zobrazí se stránka **Vytvoření uživatelského certifikátu** .
4. Na panelu **Vytvořit uživatelský certifikát** vyplňte povinná pole pod informacemi o certifikátu pro **Název organizace**, **Stav** nebo **kraj**, **Země** nebo **region**. Volitelně zadejte hodnoty do polí **Organizační jednotka** a **Lokalita** nebo **Město** . Klepněte na tlačítko **Pokračovat**.  
**Obecný název** je automaticky nastaven na ID uživatele, se kterým jste přihlášení do systému iSeries .
5. Na dalším panelu **Vytvořit uživatelský certifikát** klepněte na **Instalovat certifikát** a klepněte na **Pokračovat**.



Zobrazí se zpráva s textem Váš osobní certifikát byl nainstalován. Měli byste uchovat záložní kopii tohoto certifikátu.

6. Klepněte na tlačítko **OK**.
7. V závislosti na internetovém prohlížeči, který jste použili pro přístup k DCM, proveďte následující kroky:
  - a) Pro Internet Explorer vyberte: **Nástroje > Možnosti internetu > karta Obsah > Tlačítko Certifikáty > Osobní karta >**. Vyberte certifikát a klepněte na tlačítko **Exportovat**.
  - b) Pro prohlížeč Mozilla Firefox vyberte volbu **Tools > Options > Advanced > Encryption tab > View Certificates button > Your Certificates tab >**. Vyberte certifikát a klepněte na tlačítko **Zálohovat**. Vyberte cestu a název souboru a klepněte na tlačítko **OK**.
8. Přeneste exportovaný certifikát do vzdáleného systému pomocí protokolu FTP v binárním formátu.
9. Přidejte exportovaný certifikát z kroku 7 do obslužného programu iKeyman v databázi klíčů.
  - a) Pokud byl certifikát uložen pomocí prohlížeče Internet Explorer, postupujte podle pokynů uvedených v části Import ze souboru Microsoft . pfx.
  - b) Pokud byl certifikát uložen pomocí prohlížeče Mozilla Firefox, postupujte podle pokynů uvedených v tématu Import osobního certifikátu do úložiště klíčů.

Během importu zkontrolujte, zda se název štítku osobního certifikátu a certifikát podepsaného mění na to, co očekává IBM MQ . Návěští musí být buď hodnota atributu IBM MQ **CERTLABL** , je-li nastavena, nebo standardní `ibmwebsphere` s připojeným názvem správce front, vše malými písmeny. Podrobnosti najdete v tématu Digitální certifikáty certifikátu .

### ***Přidání certifikátů serveru do úložiště klíčů v systému IBM i***

Postupujte podle této procedury a přidejte požadovaný certifikát do úložiště klíčů.

### **Informace o této úloze**

Poté, co certifikační autorita odešle nový certifikát serveru, jej přidáte do úložiště certifikátů, ze kterého jste požadavek vygenerovali. Pokud CA odešle certifikát jako část e-mailové zprávy, zkopírujte tento certifikát do samostatného souboru.

#### **Poznámka:**

- Tuto proceduru nemusíte provádět, pokud je certifikát serveru podepsán vaším lokálním CA.
- Dříve než importujete certifikát serveru ve formátu PKCS #12 do DCM, musíte nejprve importovat odpovídající certifikát CA.

Chcete-li přijmout certifikát serveru do úložiště certifikátů správce front, postupujte takto:

### **Postup**

1. Přistupte k rozhraní DCM, jak je popsáno v tématu “Přístup k DCM” na stránce 262.
2. V kategorii úloh **Spravovat certifikáty** v navigačním panelu klepněte na volbu **Importovat certifikát**. Stránka Importovat certifikát se zobrazí v rámci úlohy.
3. Vyberte přepínač pro daný typ certifikátu a klepněte na tlačítko **Pokračovat**. V rámci úlohy se zobrazí buď stránka Import serveru, Certifikát klienta, nebo stránka Import certifikátu certifikační autority (CA).
4. V poli **Importovat soubor** zadejte název souboru certifikátu, který chcete importovat, a klepněte na **Pokračovat**. Produkt DCM automaticky určí formát souboru.
5. Je-li certifikátem certifikát **Server nebo klient** , zadejte heslo do rámce úloh a klepněte na tlačítko **Pokračovat**. Produkt DCM vás informuje o tom, že certifikát byl importován.

## **Export certifikátu z úložiště klíčů v systému IBM i**

Export certifikátu exportuje jak veřejný, tak soukromý klíč. Tato akce by měla být přijímána s extrémní opatrností, protože předání na soukromý klíč by zcela ohrozilo vaši bezpečnost.

### **Než začnete**

Sdílíte-li uživatelský certifikát s jiným uživatelem, vyměňujete veřejné klíče. Tento proces je popsán v tématu **Úloha 5. Sdílení certifikátů** v příručce Quick Start Guide for IBM MQ AMS on SYSTÉM UNIX . Když exportujete certifikát, jak je popsáno zde, exportujete veřejný i soukromý klíč. Tato akce by měla být přijímána s extrémní opatrností, protože předání na soukromý klíč by zcela ohrozilo vaši bezpečnost.

### **Informace o této úloze**

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

### **Postup**

1. Přistupte k rozhraní DCM, jak je popsáno v tématu [“Přístup k DCM”](#) na stránce 262.
2. V navigačním panelu klepněte na **Výběr úložiště certifikátů**.  
V rámci úlohy se zobrazí stránka Výběr úložiště certifikátů.
3. Vyberte úložiště certifikátů, které chcete použít, a klepněte na **Pokračovat**.
4. Volitelné: Pokud jste v kroku 3 vybrali **\*SYSTEM** , zadejte heslo do systémového úložiště a klepněte na **Pokračovat**.
5. Volitelné: Pokud jste v kroku 3 vybrali volbu **Jiná systémová paměť certifikátů** , v poli **Cesta a název souboru úložiště certifikátů** zadejte cestu k souboru IFS a název souboru, který jste nastavili při vytváření paměti certifikátů, a zadejte heslo do pole **Heslo úložiště certifikátů** . Pak klepněte na **Pokračovat**
6. V kategorii úloh **Spravovat certifikáty** v navigačním panelu klepněte na volbu **Exportovat certifikát**.  
Stránka Export certifikátu se zobrazí v rámci úlohy.
7. Vyberte přepínač pro daný typ certifikátu a klepněte na tlačítko **Pokračovat**.  
V rámci úlohy se zobrazí buď stránka Export Server, nebo stránka certifikátu klienta, nebo stránka certifikátu exportu certifikační autority (CA).
8. Vyberte certifikát, který chcete exportovat.
9. Vyberte přepínač, abyste uvedli, zda chcete exportovat certifikát do souboru nebo přímo do jiného úložiště certifikátů.
10. Pokud jste vybrali exportování certifikátu serveru nebo klienta do souboru, zadejte následující informace:
  - Cesta a název souboru umístění, do kterého chcete uložit exportovaný certifikát.
  - Pro osobní certifikát se jedná o heslo, které se používá k zašifrování exportovaného certifikátu a vydání na cílovém systému. Pro certifikáty CA není třeba zadávat heslo.
11. Pokud jste vybrali export certifikátu přímo do jiného úložiště certifikátů, určete cílové úložiště certifikátů a jeho heslo.
12. Klepněte na tlačítko **Pokračovat**.

## **Import certifikátu do úložiště klíčů v systému IBM i**

Chcete-li importovat certifikát, postupujte podle této procedury.

### **Než začnete**

Než nainportujete osobní certifikát ve formátu PKCS #12 do DCM, musíte nejprve importovat odpovídající certifikát CA.

### **Informace o této úloze**

Proveďte tyto kroky na počítači, na který chcete importovat certifikát.

## Postup

1. Přistupte k rozhraní DCM, jak je popsáno v tématu [“Přístup k DCM”](#) na stránce 262.
2. V navigačním panelu klepněte na **Výběr úložiště certifikátů**.  
V rámci úlohy se zobrazí stránka Výběr úložiště certifikátů.
3. Vyberte úložiště certifikátů, které chcete použít, a klepněte na **Pokračovat**.
4. Volitelné: Pokud jste v kroku 3 vybrali **\*SYSTEM**, zadejte heslo do systémového úložiště a klepněte na **Pokračovat**.
5. Volitelné: Pokud jste v kroku 3 vybrali volbu **Jiná systémová paměť certifikátů**, v poli **Cesta a název souboru úložiště certifikátů** zadejte cestu k souboru IFS a název souboru, který jste nastavili při vytváření paměti certifikátů, a zadejte heslo do pole **Heslo úložiště certifikátů**. Pak klepněte na **Pokračovat**.
6. V kategorii úloh **Spravovat certifikáty** v navigačním panelu klepněte na volbu **Importovat certifikát**.  
Stránka Importovat certifikát se zobrazí v rámci úlohy.
7. Vyberte přepínač pro daný typ certifikátu a klepněte na tlačítko **Pokračovat**.  
V rámci úlohy se zobrazí buď stránka Import serveru, Certifikát klienta, nebo stránka Import certifikátu certifikační autority (CA).
8. V poli **Importovat soubor** zadejte název souboru certifikátu, který chcete importovat, a klepněte na **Pokračovat**.  
Produkt DCM automaticky určí formát souboru.
9. Je-li certifikátem certifikát **Server nebo klient**, zadejte heslo do rámce úloh a klepněte na tlačítko **Pokračovat**. Produkt DCM vás informuje o tom, že certifikát byl importován.

## Odebrání certifikátů v produktu IBM i

Tento postup slouží k odebrání osobních certifikátů.

## Postup

1. Přistupte k rozhraní DCM, jak je popsáno v tématu [“Přístup k DCM”](#) na stránce 262.
2. V navigačním panelu klepněte na **Výběr úložiště certifikátů**.  
V rámci úlohy se zobrazí stránka Výběr úložiště certifikátů.
3. Označte zaškrtačací políčko **Další systémové úložiště certifikátů** a klepněte na **Pokračovat**.  
Zobrazí se stránka Paměť certifikátů a heslo.
4. Do pole **Cesta k úložišti certifikátů a název souboru** zadejte cestu k souboru IFS a název souboru, který jste nastavili při vytváření paměti certifikátů.
5. Do pole **Heslo úložiště certifikátů** zadejte heslo. Klepněte na tlačítko **Pokračovat**.  
V rámci úlohy se zobrazí stránka Aktuální úložiště certifikátů.
6. V kategorii úloh **Správa certifikátů** v navigačním panelu klepněte na volbu **Odstranit certifikát**.  
V rámci úlohy se zobrazí stránka Potvrzení odstranění certifikátu.
7. Vyberte certifikát, který chcete odstranit. Klepněte na tlačítko **Odstranit**.
8. Klepnutím na tlačítko **Ano** potvrďte, že chcete odstranit certifikát. Jinak klepněte na volbu **Ne**.  
Produkt DCM vás informuje o tom, že certifikát odstranil.

## Použití úložiště certifikátů \*SYSTEM pro jednosměrné ověření v systému IBM i

Postupujte podle těchto pokynů, chcete-li nastavit jednosměrné ověření.

## Než začnete

- Vytvořte správce front, kanály a přenosové fronty.
- Vytvořte certifikát serveru nebo klienta ve správci front serveru.
- Přeneste certifikát CA do správce front klienta a naimportuje jej do úložiště klíčů.

- Spusťte modul listener na správci front serveru a klienta.

## Informace o této úloze

Chcete-li použít jednosměrnou autentizaci, pomocí počítače se serverem IBM i jako SSL server nastavte parametr SSLKEYR (Secure Key Repository) na \*SYSTEM. Toto nastavení registruje správce front produktu IBM MQ jako aplikaci. Poté můžete přiřadit certifikát správci front, který povolí jednosměrné ověření.

Soukromá úložiště klíčů můžete také použít k implementaci jednosměrného ověření vytvořením fiktivního certifikátu pro správce front klienta v úložišti klíčů.

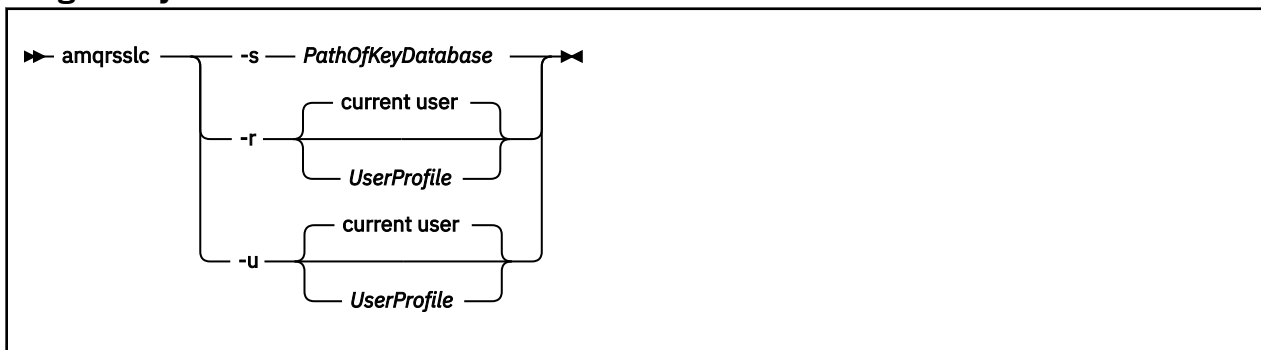
## Postup

1. Na serveru a ve správci front klienta proveďte následující kroky:
  - a) Upravte správce front tak, aby nastavil parametr SSLKEYR zadáním příkazu CHGMQM QMNAME(SSL) SSLKEYR(\*SYSTEM).
  - b) Založit heslo pro výchozí úložiště klíčů zadáním příkazu CHGMQM QMNAME(SSL) SSLKEYRPWD('xxxxxxx').  
Heslo musí být v jednoduchých uvozovkách.
  - c) Upravte kanály tak, aby měly v parametru SSLCIPHERE správnou položku CipherSpec .
  - d) Aktualizujte zabezpečení SSL zadáním příkazu RFRMQMAUT QMNAME(QMGRNAME) TYPE(\*SSL).
2. Přiřaďte certifikát ke správci front serveru pomocí produktu DCM, jak je uvedeno:
  - a) Přistupte k rozhraní DCM, jak je popsáno v tématu [“Přístup k DCM”](#) na stránce 262.
  - b) V navigačním panelu klepněte na **Výběr úložiště certifikátů**.  
V rámci úlohy se zobrazí stránka Výběr úložiště certifikátů.
  - c) Vyberte paměť certifikátů \*SYSTEM a klepněte na **Pokračovat**.
  - d) V levém panelu rozbalte volbu **Správa aplikací**.
  - e) Vyberte definici **Zobrazit aplikaci** a zkontrolujte, zda byl správce front registrován jako aplikace.  
SSL (WMQ) je uveden v tabulce.
  - f) Vyberte **Aktualizovat přiřazení certifikátu**.
  - g) Vyberte **Server** a klepněte na **Pokračovat**.
  - h) Vyberte QMGRNAME (WMQ) a klepněte na **Aktualizovat přiřazení certifikátu**.
  - i) Vyberte certifikát a klepněte na **Přiřadit nový certifikát**. Otevře se okno se zprávou, že certifikát byl přiřazen k aplikaci.

## Obslužný program IBM MQ SSL Client (amqrsslc) pro IBM i

Obslužný program klienta zabezpečení SSL produktu IBM MQ (amqrsslc) pro produkt IBM i je používán produktem IBM MQ MQI client v systémech IBM i k registraci nebo zrušení registrace profilu uživatele klienta nebo k uložení hesla úložiště certifikátů. Obslužný program může být spuštěn pouze uživatelem s profilem se zvláštním oprávněním \*ALLOBJ nebo členem QMQMADM, který má volby pro vytvoření nebo odstranění registrace aplikací v DCM (Digital Certificate Manager).

## Diagram syntaxe



## Registrace profilu uživatele klienta

Pokud IBM MQ MQI client používá paměť certifikátů \*SYSTEM, musíte registrovat uživatelský profil klienta (přihlašovací jméno uživatele) pro použití jako aplikace s produktem [Digital Certificate Manager \(DCM\)](#).

Pokud chcete registrovat uživatelský profil klienta, spusťte program **amqrsslc** s volbou `-r` s volbou *UserProfile*. Profil uživatele použitý při volání **amqrsslc** musí mít oprávnění \*USE. Zadání *UserProfile* s volbou `-r` registruje *UserProfile* jako serverovou aplikaci s jedinečným popisem aplikace QIBM\_WEBSPPHERE\_MQ\_ < *UserProfile* > a popisem s popisem < *UserProfile* > (WMQ). Tato serverová aplikace se pak zobrazí v DCM a můžete přiřadit této aplikaci jakýkoli serverový nebo klientský certifikát v systémovém úložišti.

**Poznámka:** Není-li profil uživatele zadán s volbou `-r`, je zaregistrován uživatelský profil uživatele, který spouští nástroj **amqrsslc**.

Následující kód používá produkt **amqrsslc** k registraci profilu uživatele. V prvním příkladu je registrován uvedený uživatelský profil; ve druhém je profil přihlášeného uživatele:

```
CALL PGM(QMQM/AMQRSSLC) PARM('-r' UserProfile)
CALL PGM(QMQM/AMQRSSLC) PARM('-r')
```

## Zrušit registraci profilu uživatele klienta

Chcete-li zrušit registraci profilu klienta, spusťte program **amqrsslc** s volbou `-u` s volbou *UserProfile*. Profil uživatele použitý při volání **amqrsslc** musí mít oprávnění \*USE. Zadání volby *UserProfile* s volbou `-u` zruší registraci *UserProfile* s označením QIBM\_WEBSPPHERE\_MQ\_ < *UserProfile* > z DCM.

**Poznámka:** Není-li profil uživatele zadán s volbou `-u`, odregistruje se uživatel, který spustil nástroj **amqrsslc**.

Následující kód používá produkt **amqrsslc** ke zrušení registrace profilu uživatele. V prvním příkladu je zadaný profil uživatele odregistrován; ve druhém je profil přihlášeného uživatele:

```
CALL PGM(QMQM/AMQRSSLC) PARM('-u' UserProfile)
CALL PGM(QMQM/AMQRSSLC) PARM('-u')
```

## Uskladovat heslo k úložišti certifikátů

Pokud IBM MQ MQI client nepoužívá paměť certifikátů \*SYSTEM a používá jiné úložiště certifikátů (to znamená, že je hodnota MQSSLKEYR nastavena na jinou hodnotu než \*SYSTEM), pak heslo databáze klíčů musí být uloženo. Použijte volbu `-s` pro uložení hesla databáze klíčů na sezavání.

V následujícím kódu je úplný název souboru úložiště certifikátů /Path/Of/KeyDatabase/MyKey.kdb:

```
CALL PGM(QMQM/AMQRSSLC) PARM('-s' '/Path/Of/KeyDatabase/MyKey')
```

Spuštění tohoto kódu využije požadavek na heslo této databáze klíčů. Toto heslo je uloženo v souboru se stejným názvem jako má databáze klíčů s příponou .sth. Tento soubor je uložen na stejné cestě jako databáze klíčů. Příklad kódu generuje soubor stash produktu /Path/0f/KeyDatabase/MyKey .sth. QMQM je vlastník uživatele a QMQMADM vlastníka skupiny pro tento soubor. QMQM a QMQMADM mají oprávnění ke čtení, oprávnění k zápisu a jiné profily mají pouze oprávnění ke čtení.

### **Kdy změny certifikátů nebo paměti certifikátů vstoupí v platnost na IBM i**

Změníte-li certifikáty v úložišti certifikátů nebo v umístění úložiště certifikátů, projeví se změny v závislosti na typu kanálu a způsobu, jakým je kanál spuštěn.

Změny certifikátů v úložišti certifikátů a v atributu úložiště klíčů se projeví v následujících situacích:

- 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.
- Když je vydán příkaz MQSC REFRESH SECURITY TYPE (SSL) k aktualizaci prostředí zabezpečení SSL produktu IBM MQ .
- Pro procesy klientské aplikace, když je zavřeno poslední připojení SSL v procesu. Další připojení SSL vyzvedne změny certifikátu.
- V případě kanálů, které jsou spuštěny 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 projevíly okamžitě, spusťte příkaz MQSC REFRESH SECURITY TYPE (SSL).

### **Konfigurace kryptografického hardwaru v systému IBM i**

Tento postup slouží ke konfiguraci šifrovacího koprocesoru 4758 PCI v systému IBM i

#### **Než začnete**

Zajistěte, aby váš uživatelský profil měl speciální oprávnění \*ALLOBJ a \*SECADM, abyste mohli konfigurovat hardware koprocesoru.

#### **Postup**

1. Přejděte do adresáře `http://machine.domain:2001` nebo `https://machine.domain:2010`, kde *machine* je název vašeho počítače.  
Zobrazí se dialogové okno s požadavkem na jméno uživatele a heslo.
2. Zadejte platný uživatelský profil a heslo produktu IBM i .
3. Na stránce AS/400 Tasks klepněte na **4758 PCI Cryptographic Coprocessor**.

#### **Jak pokračovat dále**

Další informace o konfiguraci šifrovacího koprocesoru 4758 PCI naleznete v *dokumentaci produktu IBM i* na adrese [IBM System i](#) a v *dokumentaci produktu IBM i*.

### **Práce se SSL nebo TLS v systémech UNIX, Linux a Windows**

V systémech UNIX, Linux a Windows je podpora zabezpečení Secure Sockets Layer (SSL) nebo TLS (Transport Layer Security) nainstalována s produktem IBM MQ.

Podrobnější informace o zásadách ověření platnosti certifikátu naleznete v tématu [Ověřování platnosti certifikátu a návrh zásad důvěryhodnosti](#).

### **Použití `runmqckm`, `runmqakm` a `strmqikm` pro správu digitálních certifikátů**

V systémech UNIX, Linux a Windows spravujte klíče a digitální certifikáty pomocí `strmqikm` (iKeyman). GUI, nebo z příkazového řádku pomocí `runmqckm` (iKeycmd) nebo `runmqakm` (GSKCapiCmd).

#### • Pro systémy **SYSTÉM UNIX a Linux** :

- Použijte příkaz `strmqikm` (iKeyman) ke spuštění grafického uživatelského rozhraní iKeyman .
- Použijte příkaz `runmqckm` (iKeycmd) k provedení úloh s rozhraním příkazového řádku iKeycmd .
- K provedení úloh s rozhraním příkazového řádku `runmqakm` použijte příkaz `runmqakm` (GSKCapiCmd). Syntaxe příkazu pro `runmqakm` je stejná jako syntaxe pro `runmqckm`.

Potřebujete-li spravovat certifikáty 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. Pouze 32bitové platformy Windows a Linux x86 jsou jediné výjimky, protože programy iKeyman a iKeycmd jsou na těchto platformách 32 bitové.

Další informace viz [GSKit: PKCS#11 and JRE addressing mode](#) .

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` .

- Použijte příkaz `runmqakm -keydb` s volbou `stashpw` nebo `stash` .

Při použití příkazu `runmqakm -keydb` tímto způsobem:

```
runmqakm -keydb -create -db key.kdb -pw secretpwd -stash
```

výsledný soubor `.sth` nemá povolené oprávnění ke čtení pro skupinu `mqm` .

Tento soubor může číst pouze tvůrce. Po vytvoření souboru pro dočasné ukládání pomocí příkazu `runmqakm` zkontrolujte oprávnění k souboru a udělte oprávnění servisnímu účtu, který spouští správce front, nebo skupině, jako je lokální `mqm`.

Chcete-li vyžádat trasování SSL v systémech UNIX, Linux nebo Windows , přečtěte si téma [strmqtrc](#).



## Související informace

[runmqckm a příkazy runmqakm](#)

### **Nastavení úložiště klíčů v systému SYSTÉM UNIX, Linuxu a Okna**

Úložiště klíčů můžete nastavit pomocí produktu **strmqikm** (iKeyman). Grafické rozhraní nebo z příkazového řádku pomocí příkazů **runmqckm** (iKeycmd) nebo **runmqakm** (GSKCapiCmd).

## Informace o této úloze

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

V systému SYSTÉM UNIX, Linuxu a Okna jsou digitální certifikáty uloženy v souboru databáze klíčů, který je spravován pomocí uživatelského rozhraní produktu **strmqikm** nebo pomocí příkazů **runmqckm** nebo **runmqakm**. Tyto digitální certifikáty mají štítky. Specifický popisec asociuje osobní certifikát se správcem front nebo IBM MQ MQI client. TLS používá tento certifikát pro účely autentizace. Na systémech SYSTÉM UNIX, Linuxu a Okna používá produkt IBM MQ hodnotu atributu **CERTLABL** (pokud je nastavena) nebo standardní `ibmwebspheremq` s připojeným jménem správce front nebo přihlašovacího ID uživatele IBM MQ MQI client, vše malými písmeny. Podrobnosti najdete v tématu [Digitální certifikáty certifikátu](#).

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

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

V systémech Windows je výchozí cesta

`MQ_INSTALLATION_PATH\qmgrs\queue_manager_name\ssl`, kde `MQ_INSTALLATION_PATH` je adresář, ve kterém je nainstalován produkt IBM MQ. Například `C:\Program Files\IBM\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 IBM MQ neexistuje žádná výchozí cesta nebo název kmene. Ulehčeně řídit přístup k tomuto souboru. Rozšíření musí být `.kdb`.

Nevytvářejte klíčová úložiště na systému souborů, který nepodporuje zámky na úrovni souboru, například NFS verze 2 na systémech Linux.

Informace o kontrole a určení názvu souboru databáze klíčů viz [“Změna umístění úložiště klíčů pro správce front v systémech UNIX, Linux nebo Windows”](#) na stránce 279. Název souboru databáze klíčů můžete zadat buď před vytvořením databázového souboru klíčů, nebo po něm.

ID uživatele, ze kterého spouštíte příkazy **strmqikm** nebo **runmqckm**, musí mít oprávnění k zápisu do adresáře, ve kterém je soubor databáze klíčů vytvořen nebo aktualizován. Pro správce front, který používá výchozí adresář `ssl`, musí být ID uživatele, ze kterého spouštíte produkt **strmqikm** nebo **runmqckm**, členem skupiny `mqm`. Pokud u produktu IBM MQ MQI clients pustíte příkaz **strmqikm** nebo **runmqckm** z jiného ID uživatele, než je ID uživatele, pod nímž je klient spuštěn, musíte změnit oprávnění k souboru, aby mohl produkt IBM MQ MQI client přistupovat k souboru databáze klíčů za běhu programu. Další informace viz [“Přístup k databázovým souborům a jejich zabezpečení v systému Windows”](#) na stránce 277 nebo [“Přístup k databázovým souborům a jejich zabezpečení v systémech SYSTÉM UNIX a Linux”](#) na stránce 277.

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



**Poznámka:** Vzhledem k této změně chování sady 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 použitými certifikáty CA. Viz [“Přidání výchozích certifikátů CA do prázdného úložiště klíčů v produktu SYSTÉM UNIX, Linuxu Okna s GSKit Verze 8.0” na stránce 278.](#)

Databázi klíčů vytvoříte buď pomocí příkazového řádku, nebo pomocí uživatelského rozhraní produktu **strmqikm** (iKeyman).

**Poznámka:** Musíte-li spravovat certifikáty TLS způsobem, který je kompatibilní se standardem FIPS-, použijte příkaz **runmqakm** . Uživatelské rozhraní produktu **strmqikm** neposkytuje volbu vyhovující FIPS.

## Postup

Vytvořte databázi klíčů pomocí příkazového řádku.

1. Spusťte některý z následujících příkazů:

- Použití **runmqckm**:

```
runmqckm -keydb -create -db filename -pw password -type cms -stash
```

- Použití **runmqakm**:

```
runmqakm -keydb -create -db filename -pw password -type cms  
-stash -fips -strong
```

kde:

**-db *název\_souboru***

Uvádí plně kvalifikovaný název souboru databáze klíčů CMS a musí mít příponu souboru `.kdb`.

**-pw *heslo***

Určuje heslo pro databázi klíčů CMS.

**-type *cms***

Uvádí typ databáze. (Pro IBM MQ musí být `cms`.)

**-stash**

Uloží heslo databáze klíčů do souboru.

**-fips**

určuje, že příkaz má být spuštěn v režimu FIPS. Při použití režimu FIPS komponenta ICC používá algoritmy, které jsou validovány FIPS 140-2. Pokud se komponenta ICC neinicializuje v režimu FIPS, příkaz **runmqakm** se nezdaří.

**-silné**

Kontroluje, zda zadané heslo splňuje minimální požadavky na odolnost hesla. Minimální požadavky na heslo jsou tyto:

- Heslo musí mít minimální délku 14 znaků.
- Heslo musí obsahovat minimálně jedno malé písmeno, jedno velké písmeno a jednu číslici nebo speciální znak. Mezi speciální znaky patří hvězdička (\*), znak dolaru (\$), symbol čísla (#) a znak procenta (%). Prostor je klasifikován jako speciální znak.
- Každý znak může v hesle nastat maximálně třikrát.
- Maximální počet dvou po sobě jdoucích znaků v hesle může být stejný.
- Všechny znaky jsou ve standardním tisknutelném znakové sadě ASCII, v rozsahu 0x20 - 0x7E.

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

2. V systémech SYSTÉM UNIX a Linux se přihlaste jako uživatel `root`. V systému Windows se přihlaste jako administrátor nebo jako člen skupiny `MQM`.
3. Spusťte uživatelské rozhraní spuštěním příkazu **strmqikm** .
4. V nabídce **Soubor databáze klíčů** klepněte na volbu **Nový**.

Otevře se nové okno.

5. Klepněte na volbu **Typ databáze klíčů** a vyberte položku **CMS** (Certificate Management System).
6. Do pole **Název souboru** zadejte název souboru.  
Toto pole již obsahuje text `key.kdb`. Pokud je váš název kmene `key`, ponechte toto pole nezměněné. Pokud jste uvedli jiný název souboru, nahraďte `key` svým kmenovým jménem. Rozšíření `.kdb` však nesmíte změnit.
7. Do pole **Umístění** zadejte cestu.

Příklad:

- Pro správce front: `/var/mqm/qmgrs/QM1/ssl` (v systémech SYSTÉM UNIX a Linux) nebo `C:\ProgramData\IBM\MQ\qmgrs\QM1\ssl` (v systémech Windows).

Cesta se musí shodovat s hodnotou atributu **SSLKeyRepository** správce front.

- Pro klienta IBM MQ: `/var/mqm/ssl` (v systémech SYSTÉM UNIX a Linux) nebo `C:\mqm\ssl` (v systémech Windows).

8. Klepněte na tlačítko **OK**.

Otevře se okno Výzva k zadání hesla.

9. Do pole **Heslo** zadejte heslo a zadejte je znovu do pole **Potvrdit heslo**.

10. Vyberte zaškrtačací políčko **Stash heslo do souboru**.

**Poznámka:** Pokud heslo neschováte, pokusy o spuštění kanálů TLS selžou, protože nemohou získat heslo potřebné pro přístup k souboru databáze klíčů.

11. Klepněte na tlačítko **OK**.

Otevře se okno Osobní certifikáty.

12. Nastavte přístupová oprávnění podle popisu v části "Přístup k databázovým souborům a jejich zabezpečení v systému Windows" na stránce 277 nebo "Přístup k databázovým souborům a jejich zabezpečení v systémech SYSTÉM UNIX a Linux" na stránce 277.

#### *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 SYSTÉM UNIX a 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 uživatelem 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.crl* a *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 -----).

**ULW** Přidání výchozích certifikátů CA do prázdného úložiště klíčů v produktu SYSTÉM UNIX, Linuxa Okna s 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 7.0 se 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 produktu strmqikm

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

1. Spusťte grafické rozhraní pomocí příkazu **strmqikm** (v systému SYSTÉM UNIX, Linuxa Okna).
2. V nabídce **Soubor databáze klíčů** klepněte na volbu **Otevřít**. Otevře se okno Otevřít.
3. Klepněte na volbu **Typ databáze klíčů** a vyberte položku **CMS** (Certificate Management System).
4. Klepněte na tlačítko **Procházet** a přejděte do adresáře, který obsahuje soubory databáze klíčů.
5. Vyberte soubor databáze klíčů, do nějž chcete přidat certifikát, tj. například *key.kdb*.
6. Klepněte na tlačítko **Otevřít**. Otevře se okno Výzva k zadání hesla.
7. Zadejte heslo, jež jste nastavili při vytvoření databáze klíčů, a klepněte na tlačítko **OK**. Název vašeho souboru databáze klíčů se zobrazuje v poli **Název souboru**.
8. V poli **Obsah databáze klíčů** vyberte položku **Certifikáty podepsaného**.
9. Klepněte na **Naplnit**. Otevře se okno Přidání certifikátu CA.
10. Certifikáty CA, které jsou k dispozici pro přidání do úložiště, jsou zobrazeny v hierarchické stromové struktuře. Vyberte položku nejvyšší úrovně pro organizaci, jejíž certifikáty CA chcete důvěřovat, abyste zobrazili úplný seznam platných certifikátů CA.
11. Vyberte certifikáty CA, kterým chcete důvěřovat ze seznamu, a klepněte na **OK**. Certifikáty se přidají do úložiště klíčů.

## z příkazového řádku,

Pomocí následujících příkazů zobrazte seznam a poté přidejte certifikáty CA pomocí produktu **runmqckm**:

- Vydejte následující příkaz, který vypíše výchozí certifikáty CA spolu s organizacemi, které je vydávají:

```
runmqckm -cert -listsigners
```

- Chcete-li přidat všechny certifikáty CA pro organizaci uvedenou v poli *label*, zadejte následující příkaz:

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

kde:

- |                     |                                      |
|---------------------|--------------------------------------|
| -db <i>filename</i> | je úplná cesta k databázi klíčů.     |
| -pw <i>password</i> | je heslo pro databázi klíčů.         |
| -label <i>label</i> | je jmenovka přiložená k certifikátu. |

**Poznámka:** Přidání certifikátu CA do úložiště klíčů vede k tomu, že produkt IBM MQ důvěřuje všem osobním certifikátům podepsaným daným certifikátem CA. Pečlivě zvažte, které certifikační autority chcete důvěřovat, a přidejte pouze sadu certifikátů CA potřebných k ověření klientů a správců. Nedoporučuje se přidávat plnou sadu výchozích certifikátů CA, pokud to není definitivní požadavek pro vaši strategii zabezpečení.

## **Vyhledání úložiště klíčů pro správce front v systémech UNIX, Linux nebo 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 MQ Explorer nebo PCF.

2. Provéřte výstup příkazu pro cestu a název stem databázového souboru klíčů.

Například

- a. na systémech SYSTÉM UNIX a Linux : /var/mqm/qmgrs/QM1/ssl/key, kde /var/mqm/qmgrs/QM1/ssl je cesta a key je název kmene
- b. na Windows: MQ\_INSTALLATION\_PATH\qmgrs\QM1\ssl\key, kde MQ\_INSTALLATION\_PATH\qmgrs\QM1\ssl je cesta a key je název kmene. MQ\_INSTALLATION\_PATH představuje adresář vysoké úrovně, ve kterém je nainstalován produkt IBM MQ.

## **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 SYSTÉM UNIX a Linux :

```
ALTER QMGR SSLKEYR('var/mqm/qmgrs/QM1/ssl/MyKey')
```

Soubor databáze klíčů má úplný název souboru: /var/mqm/qmgrs/QM1/ssl/MyKey.kdb

zapWindows:

```
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 IBM MQ nebo PCF.

Změníte-li umístění souboru databáze klíčů správce front, nebudou certifikáty přeneseny ze starého umístění. Je-li klíčovým databázovým souborem, k němuž nyní přistupujete, nový soubor databáze klíčů, musíte jej naplnit daty CA a osobními certifikáty, které potřebujete, jak je popsáno v tématu [“Import osobního certifikátu do úložiště klíčů v systému SYSTÉM UNIX, Linuxu Okna”](#) na stránce 294.

## **Nalezení klíčového úložiště pro IBM MQ MQI client v systémech UNIX, Linux a Windows .**

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

Proveřte proměnnou prostředí MQSSLKEYR a vyhledejte umístění souboru databáze klíčů pro produkt IBM MQ MQI client. Příklad:

```
echo $MQSSLKEYR
```

Zkontrolujte také svou aplikaci, protože název souboru databáze klíčů lze také nastavit v rámci volání MQCONN, jak je popsáno v tématu [“Zadání umístění úložiště klíčů pro zařízení IBM MQ MQI client v systémech UNIX, Linux nebo Windows”](#) na stránce 280. Hodnota nastavená ve volání MQCONN přepíše hodnotu proměnné MQSSLKEYR.

### **Zadání umístění úložiště klíčů pro zařízení IBM MQ MQI client v systémech UNIX, Linux nebo Windows**

Pro IBM MQ MQI client 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 pro produkt IBM MQ MQI client můžete určit dvěma způsoby:

- Nastavení proměnné prostředí MQSSLKEYR. Například na systémech SYSTÉM UNIX a Linux :

```
export MQSSLKEYR=/var/mqm/ssl/key
```

Soubor databáze klíčů má plně kvalifikovaný název souboru:

```
/var/mqm/ssl/key.kdb
```

zapWindows:

```
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 MQCONN při volání aplikace MQCONN. Další informace o použití struktury MQSCO v MQCONN najdete v tématu [Přehled pro MQSCO](#).

### **Když se změny certifikátů nebo paměti certifikátů stanou platnými v 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 spuštěny jako podprocesy procesu fondu procesů (amqrmppa), je-li proces sdružování procesů spuštěn nebo restartován a nejprve spustí kanál SSL. Pokud proces

sdužování 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 projevíly okamžitě, spusťte příkaz MQSC REFRESH SECURITY TYPE (SSL).

Prostředí IBM MQ zabezpečení SSL můžete aktualizovat také pomocí příkazů IBM MQ Explorer nebo PCF.

## **ULW** Vytvoření osobního certifikátu podepsaného sebou samým na serveru **SYSTÉM UNIX, Linuxa Okna**

Certifikát s automatickým podpisem můžete vytvořit pomocí **strmqikm** (iKeyman) GUI, nebo z příkazového řádku pomocí **runmqckm** (iKeycmd) nebo **runmqakm** (GSKCapiCmd).

**Poznámka:** Produkt IBM MQ nepodporuje algoritmy SHA-3 nebo SHA-5 . Můžete použít názvy algoritmů digitálního podpisu SHA384WithRSA a SHA512WithRSA , protože oba algoritmy jsou členy řady SHA-2 .

Názvy algoritmů digitálního podpisu SHA3WithRSA a SHA5WithRSA jsou zamítnuty, protože se jedná o zkrácený tvar SHA384WithRSA a SHA512WithRSA .

Další informace o důvodech použití certifikátů s vlastním podpisem naleznete v tématu [Použití certifikátů podepsaných držitelem pro vzájemné ověření dvou správců front](#).

Ne všechny digitální certifikáty lze použít se všemi CipherSpecs. Ujistěte se, že jste vytvořili certifikát, který je kompatibilní se specifikacemi CipherSpecs , které potřebujete použít. Produkt IBM MQ podporuje tři různé typy CipherSpec. Podrobné informace naleznete v tématu “[Interoperabilita Eliptické křivky a RSA CipherSpecs](#)” na stránce 45 v tématu “[Digitální certifikáty a kompatibilita CipherSpec v produktu IBM MQ](#)” na stránce 44 .

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.

Pokud používáte:

- Grafické rozhraní, viz “[Použití uživatelského rozhraní produktu strmqikm](#)” na stránce 281
- Příkazový řádek, viz “[z příkazového řádku,](#)” na stránce 282

## **ULW** Použití uživatelského rozhraní produktu **strmqikm**

Osobní certifikát můžete vytvořit pomocí produktu **strmqikm** (iKeyman). -GII.

### Informace o této úloze

**strmqikm** neposkytuje volbu vyhovující FIPS. Potřebujete-li spravovat certifikáty TLS způsobem, který je kompatibilní se standardem FIPS-, použijte příkaz **runmqakm** .

### Postup

Chcete-li vytvořit osobní certifikát pro správce front nebo produkt IBM MQ MQI client pomocí grafického uživatelského rozhraní, proveďte následující kroky:

1. Spusťte grafické rozhraní pomocí příkazu **strmqikm** .
2. V nabídce **Soubor databáze klíčů** klepněte na volbu **Otevřít**.  
Zobrazí se okno **Otevřít** .
3. Klepněte na volbu **Typ databáze klíčů** a vyberte položku **CMS** (Certificate Management System).
4. Klepněte na tlačítko **Procházet** a přejděte do adresáře, který obsahuje soubory databáze klíčů.

5. Vyberte soubor databáze klíčů, ze kterého chcete generovat požadavek, například `key.kdb`.
6. Klepněte na tlačítko **OK**.  
Otevře se okno **Výzva k zadání hesla**.
7. Zadejte heslo, jež jste nastavili při vytvoření databáze klíčů, a klepněte na tlačítko **OK**.  
Název databázového souboru databáze se zobrazí v poli **Název souboru**.
8. V nabídce **Vytvořit** klepněte na **Nový certifikát podepsaný svým držitelem**. Zobrazí se okno Vytvoření nového certifikátu podepsaného sám sebou.
9. Do pole **Jmenovka klíče** zadejte jmenovku certifikátu.  
Jmenovka je buď hodnota atributu **CERTLABL**, je-li nastavena, nebo standardní `ibmwebspheremq` s připojeným jménem správce front nebo IBM MQ MQI client ID uživatele pro přihlášení, vše malými písmeny. Podrobnosti najdete v tématu [Digitální certifikáty certifikátu](#).
10. Zadejte nebo vyberte hodnotu pro libovolné pole v poli **Rozlišovací jméno** nebo kterékoliv z polí **Alternativní jméno subjektu**.
11. U zbývajících polí buď přijměte výchozí hodnoty, nebo zadejte nové hodnoty nebo vyberte nové hodnoty.  
Další informace o rozlišujících názvech naleznete v tématu [“Rozlišující názvy”](#) na stránce 11.
12. Klepněte na tlačítko **OK**.  
Seznam **Osobní certifikáty** zobrazuje štítek osobního certifikátu podepsaného sebou samým, který jste vytvořili sami.

## Jak pokračovat dále

Odešlete žádost o certifikát certifikační autoritě. Další informace viz [“Přijímání osobních certifikátů do úložiště klíčů v systému SYSTÉM UNIX, Linuxa Okna”](#) na stránce 288.

 z příkazového řádku,

Osobní certifikát můžete vytvořit z příkazového řádku pomocí příkazů **runmqckm** (iKeycmd) nebo **runmqakm** (GSKCapiCmd). Potřebujete-li spravovat certifikáty SSL nebo TLS způsobem, který je kompatibilní se standardem FIPS-, použijte příkaz **runmqakm**.

## Informace o této úloze

### Postup

Vytvořte osobní certifikát podepsaný držitelem pomocí příkazu `GSKCapiCmd` (**runmqckm** nebo **runmqakm**).

- Použití **runmqckm** na SYSTÉM UNIX, Linuxa Okna:

```
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
```



kde:

**-db název\_souboru**

Uvádí plně kvalifikovaný název souboru databáze klíčů CMS.

**-pw heslo**

Určuje heslo pro databázi klíčů CMS.

**-label popisek**

Určuje jmenovku klíče připojenou k certifikátu. Návěští je buď hodnota atributu **CERTLABL** , pokud je nastavena, nebo standardní `ibmwebspheremq` s názvem správce front nebo přihlašovacím jménem uživatele IBM MQ MQI client , které jsou připojeny, vše malými písmeny. Podrobnosti viz [“Digitální certifikáty certifikátu, základní informace o požadavcích”](#) na stránce 25.

**-dn rozlišující\_název**

Určuje rozlišující název X.509 uzavřený ve dvojitých uvozovkách. Je povinný alespoň jeden atribut. Můžete zadat více atributů OU a DC.

**Poznámka:** Nástroje `runmqckm` a `runmqakm` odkazují na atribut PSČ jako `POSTALCODE`, nikoli na `PC`. Vždy zadejte `POSTALCODE` do parametru **-dn** , když použijete tyto příkazy správy certifikátů k vyžádání certifikátů s poštovním směrovači.

**-size velikost\_klíče**

Určuje velikost klíče. Pokud používáte produkt `runmqckm`, hodnota může být 512 nebo 1024. Pokud používáte produkt `runmqakm`, hodnota může být 512, 1024 nebo 2048.

**x509version verze**

Verze certifikátu X.509 , který má být vytvořen. Hodnota může být 1, 2 nebo 3. Výchozí hodnota je 3.

**-file název\_souboru**

Určuje název souboru pro žádost o certifikát.

**-expire dny**

Doba vypršení platnosti ve dnech certifikátu. Předvolba je 365 dní pro certifikát.

**-fips**

určuje, že příkaz má být spuštěn v režimu FIPS. Je použita pouze komponenta FIPS ICC a tato komponenta musí být úspěšně inicializována v režimu FIPS. V režimu FIPS komponenta ICC používá algoritmy ověřené dle standardu FIPS 140-2. Není-li komponenta ICC inicializována v režimu FIPS, příkaz `runmqakm` selže.

**-sig\_alg**

Pro `runmqckm` uvádí asymetrický podpisový algoritmus použitý pro vytvoření dvojice klíčů položky. The value can be, MD2\_WITH\_RSA, MD2WithRSA, MD5\_WITH\_RSA, MD5WithRSA, SHA1WithDSA, SHA1WithECDSA, SHA1WithRSA, SHA2/ECDSA, SHA224WithECDSA, SHA256\_WITH\_RSA, SHA256WithECDSA, SHA256WithRSA, SHA2WithECDSA, SHA3/ECDSA, SHA384\_WITH\_RSA, SHA384WithECDSA, SHA384WithRSA, SHA3WithECDSA, SHA5/ECDSA, SHA512\_WITH\_RSA, SHA512WithECDSA, SHA512WithRSA, SHA5WithECDSA, SHA\_WITH\_DSA, SHA\_WITH\_RSA, SHAWithDSA, SHAWithRSA. Výchozí hodnota je SHA1WithRSA.

**-sig\_alg**

Pro produkt `runmqakm` určuje algoritmus hašování použitý při vytváření žádosti o certifikát. Tento algoritmus hašování se používá k vytvoření podpisu přidruženého k nově vytvořené žádosti o certifikát. The value can be md5, MD5\_WITH\_RSA, MD5WithRSA, SHA\_WITH\_DSA, SHA\_WITH\_RSA, sha1, SHA1WithDSA, SHA1WithECDSA, SHA1WithRSA, sha224, SHA224\_WITH\_RSA, SHA224WithDSA, SHA224WithECDSA, SHA224WithRSA, sha256, SHA256\_WITH\_RSA, SHA256WithDSA, SHA256WithECDSA, SHA256WithRSA, SHA2WithRSA, sha384, SHA384\_WITH\_RSA, SHA384WithECDSA, SHA384WithRSA, sha512, SHA512\_WITH\_RSA, SHA512WithECDSA, SHA512WithRSA, SHAWithDSA, SHAWithRSA, EC\_ecdsa\_with\_SHA1, EC\_ecdsa\_with\_SHA224, EC\_ecdsa\_with\_SHA256, EC\_ecdsa\_with\_SHA384, or EC\_ecdsa\_with\_SHA512. Výchozí hodnota je SHA1WithRSA.

**-san\_dnsname DNS\_názvy**

Určuje seznam názvů DNS oddělených čárkami pro vytvářené položka, které jsou odděleny čárkami nebo mezerami jako oddělovači.



### **-san\_emailaddr e-mailové\_adresy**

Určuje seznam e-mailových adres oddělených čárkami pro vytvářený záznam, oddělený čárkami nebo mezerami jako oddělovači.

### **-san\_ipaddr adresa\_IP**

Určuje seznam adres IP oddělených čárkami pro vytvářený záznam, oddělený čárkami nebo mezerami jako oddělovači.

## **Jak pokračovat dále**

Odešlete žádost o certifikát certifikační autoritě. Další informace viz [“Přijímání osobních certifikátů do úložiště klíčů v systému SYSTÉM UNIX, Linuxa Okna”](#) na stránce 288.

### **ULW Požádání o osobní certifikát v systému SYSTÉM UNIX, Linuxa Okna**

Osobní certifikát můžete požádat pomocí produktu **strmqikm** (iKeyman) Grafické rozhraní nebo z příkazového řádku pomocí příkazů **runmqckm** (iKeycmd) nebo **runmqakm** (GSKCapiCmd). Potřebujete-li spravovat certifikáty SSL nebo TLS způsobem, který je kompatibilní se standardem FIPS-, použijte příkaz **runmqakm**.

## **Informace o této úloze**

Osobní certifikát můžete požádat buď pomocí grafického uživatelského rozhraní produktu **strmqikm**, nebo z příkazového řádku, a to s následujícími úvahami:

- Produkt IBM MQ nepodporuje algoritmy SHA-3 nebo SHA-5 . Můžete použít názvy algoritmů digitálního podpisu SHA384WithRSA a SHA512WithRSA , protože oba algoritmy jsou členy řady SHA-2 .
- Názvy algoritmů digitálního podpisu SHA3WithRSA a SHA5WithRSA jsou zamítnuty, protože se jedná o zkrácený tvar SHA384WithRSA a SHA512WithRSA .
- Ne všechny digitální certifikáty lze použít se všemi CipherSpecs. Ujistěte se, že požadujete certifikát kompatibilní se specifikacemi CipherSpecs , které potřebujete použít. Produkt IBM MQ podporuje tři různé typy CipherSpec. Podrobné informace naleznete v tématu [“Interoperabilita Eliptické křivky a RSA CipherSpecs”](#) na stránce 45 v tématu [“Digitální certifikáty a kompatibilita CipherSpec v produktu IBM MQ”](#) na stránce 44 .
- 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 302.

Pokud používáte:

- Grafické rozhraní, viz [“Použití uživatelského rozhraní produktu strmqikm”](#) na stránce 284
- Příkazový řádek, viz [“z příkazového řádku,”](#) na stránce 285

### **ULW Použití uživatelského rozhraní produktu strmqikm**

Osobní certifikát můžete požádat pomocí produktu **strmqikm** (iKeyman) Grafické rozhraní nebo z příkazového řádku pomocí příkazů **runmqckm** (iKeycmd) nebo **runmqakm** (GSKCapiCmd). Potřebujete-li spravovat certifikáty SSL nebo TLS způsobem, který je kompatibilní se standardem FIPS-, použijte příkaz **runmqakm**.

## **Informace o této úloze**

**strmqikm** neposkytuje volbu vyhovující FIPS. Potřebujete-li spravovat certifikáty TLS způsobem, který je kompatibilní se standardem FIPS-, použijte příkaz **runmqakm**.

## Postup

Chcete-li požádat o osobní certifikát pomocí uživatelského rozhraní iKeyman , proveďte následující kroky:

1. Spusťte uživatelské rozhraní pomocí příkazu **strmqikm** .
2. V nabídce **Soubor databáze klíčů** klepněte na volbu **Otevřít**.  
Otevře se okno **Otevřít**.
3. Klepněte na volbu **Typ databáze klíčů** a vyberte položku **CMS** (Certificate Management System).
4. Klepněte na tlačítko **Procházet** a přejděte do adresáře, který obsahuje soubory databáze klíčů.
5. Vyberte soubor databáze klíčů, ze kterého chcete generovat požadavek, například key . kdb.
6. Klepněte na tlačítko **Otevřít**.  
Otevře se okno **Výzva k zadání hesla** .
7. Zadejte heslo, jež jste nastavili při vytvoření databáze klíčů, a klepněte na tlačítko **OK**.  
Název databázového souboru databáze se zobrazí v poli **Název souboru** .
8. V nabídce **Vytvořit** klepněte na **Nový požadavek na certifikát**. Otevře se okno **Vytvořit nový klíč a žádost o certifikát** .
9. Do pole **Jmenovka klíče** zadejte jmenovku certifikátu.  
Jmenovka je buď hodnota atributu **CERTLABL** , je-li nastavena, nebo standardní `ibmwebsphermq` s připojeným jménem správce front nebo IBM MQ MQI client ID uživatele pro přihlášení, vše malými písmeny. Podrobnosti najdete v tématu [Digitální certifikáty certifikátu](#) .
10. Zadejte nebo vyberte hodnotu pro libovolné pole v poli **Rozlišovací jméno** nebo kterékoli 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 popis nové žádosti o osobní certifikát, kterou jste vytvořili. Požadavek na certifikát je uložen v souboru, který jste zvolili v kroku [“11”](#) na stránce 285.
14. Vyžádejte si nový osobní certifikát odesláním souboru certifikační autoritě (CA) nebo zkopírováním souboru do formuláře požadavku na webovém serveru pro CA.

**ULW** z příkazového řádku,

Můžete požádat o osobní certifikát z příkazového řádku pomocí příkazů **runmqckm** (iKeycmd) nebo **runmqakm** (GSKCapiCmd). Potřebujete-li spravovat certifikáty SSL nebo TLS způsobem, který je kompatibilní se standardem FIPS-, použijte příkaz **runmqakm** .

## Postup

Požádejte o osobní certifikát pomocí příkazu **runmqckm** nebo **runmqakm** (GSKCapiCmd).

- Použití **runmqckm**:

```
runmqckm -certreq -create -db filename -pw  
password -label label  
-dn distinguished_name -size key_size  
-file filename -sig_alg algorithm
```

Místo `-dn distinguished_name` můžete použít `-san_dsname DNS_names`, `-san_emailaddr email_addresses` nebo `-san_ipaddr IP_addresses`.

- Použití **runmqakm**:

```
runmqakm -certreq -create -db filename -pw
password -label label
        -dn distinguished_name -size key_size
        -file filename -fips -sig_alg algorithm
```

kde:

**-db název\_souboru**

Uvádí plně kvalifikovaný název souboru databáze klíčů CMS.

**-pw heslo**

Určuje heslo pro databázi klíčů CMS.

**-label popisek**

Určuje jmenovku klíče připojenou k certifikátu. Návěští je buď hodnota atributu **CERTLABL**, pokud je nastavena, nebo standardní `ibmwebspheremq` s názvem správce front nebo přihlašovacím jménem uživatele IBM MQ MQI client, které jsou připojeny, vše malými písmeny. Podrobnosti viz [“Digitální certifikáty certifikátu, základní informace o požadavcích”](#) na stránce 25.

**-dn rozlišující\_název**

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

**Poznámka:** Nástroje **runmqckm** a **runmqakm** odkazují na atribut PSČ jako POSTALCODE, nikoli na PC. Vždy zadejte POSTALCODE do parametru **-dn**, když použijete tyto příkazy správy certifikátů k vyžádání certifikátů s poštovním směrovači.

**-size velikost\_klíče**

Určuje velikost klíče. Pokud používáte produkt **runmqckm**, hodnota může být 512 nebo 1024. Pokud používáte produkt **runmqakm**, hodnota může být 512, 1024 nebo 2048.

**-file název\_souboru**

Určuje název souboru pro žádost o certifikát.

**-fips**

určuje, že příkaz má být spuštěn v režimu FIPS. Při použití režimu FIPS komponenta ICC používá algoritmy, které jsou validovány FIPS 140-2. Pokud se komponenta ICC neinicializuje v režimu FIPS, příkaz **runmqakm** se nezdaří.

**-sig\_alg**

Pro **runmqckm** uvádí asymetrický podpisový algoritmus použitý pro vytvoření dvojice klíčů položky. The value can be, MD2\_WITH\_RSA, MD2WithRSA, MD5\_WITH\_RSA, MD5WithRSA, SHA1WithDSA, SHA1WithECDSA, SHA1WithRSA, SHA2/ECDSA, SHA224WithECDSA, SHA256\_WITH\_RSA, SHA256WithECDSA, SHA256WithRSA, SHA2WithECDSA, SHA3/ECDSA, SHA384\_WITH\_RSA, SHA384WithECDSA, SHA384WithRSA, SHA3WithECDSA, SHA5/ECDSA, SHA512\_WITH\_RSA, SHA512WithECDSA, SHA512WithRSA, SHA5WithECDSA, SHA\_WITH\_DSA, SHA\_WITH\_RSA, SHAWithDSA, SHAWithRSA. Výchozí hodnota je SHA1WithRSA.

**-sig\_alg**

Pro produkt **runmqakm** určuje algoritmus hašování použitý při vytváření žádosti o certifikát. Tento algoritmus hašování se používá k vytvoření podpisu přidruženého k nově vytvořené žádosti o certifikát. The value can be md5, MD5\_WITH\_RSA, MD5WithRSA, SHA\_WITH\_DSA, SHA\_WITH\_RSA, sha1, SHA1WithDSA, SHA1WithECDSA, SHA1WithRSA, sha224, SHA224\_WITH\_RSA, SHA224WithDSA, SHA224WithECDSA, SHA224WithRSA, sha256, SHA256\_WITH\_RSA, SHA256WithDSA, SHA256WithECDSA, SHA256WithRSA, SHA2WithRSA, sha384, SHA384\_WITH\_RSA, SHA384WithECDSA, SHA384WithRSA, sha512, SHA512\_WITH\_RSA, SHA512WithECDSA, SHA512WithRSA, SHAWithDSA, SHAWithRSA, EC\_ecdsa\_with\_SHA1, EC\_ecdsa\_with\_SHA224, EC\_ecdsa\_with\_SHA256, EC\_ecdsa\_with\_SHA384, or EC\_ecdsa\_with\_SHA512. Výchozí hodnota je SHA1WithRSA.

**-san\_dnsname DNS\_názvy**

Určuje seznam názvů DNS oddělených čárkami pro vytvářená položka, které jsou odděleny čárkami nebo mezerami jako oddělovači.

### **-san\_emailaddr e-mailové\_adresy**

Určuje seznam e-mailových adres oddělených čárkami pro vytvářený záznam, oddělený čárkami nebo mezerami jako oddělovači.

### **-san\_ipaddr adresa\_IP**

Určuje seznam adres IP oddělených čárkami pro vytvářený záznam, oddělený čárkami nebo mezerami jako oddělovači.

## **Jak pokračovat dále**

Odešlete žádost o certifikát certifikační autoritě. Další informace viz [“Přijímání osobních certifikátů do úložiště klíčů v systému SYSTÉM UNIX, Linuxa Okna”](#) na stránce 288.

## **ULW Obnova existujícího osobního certifikátu v systému SYSTÉM UNIX, Linuxa Okna**

Osobní certifikát můžete obnovit pomocí produktu **strmqikm** (iKeyman). Grafické rozhraní nebo z příkazového řádku pomocí příkazů **runmqckm** (iKeycmd) nebo **runmqakm** (GSKCapiCmd).

## **Informace o této úloze**

Máte-li požadavek používat větší velikosti klíčů pro vaše osobní certifikáty, nemůžete obnovit existující certifikát. You must replace your existing key by following the steps described in [“Požádání o osobní certifikát v systému SYSTÉM UNIX, Linuxa Okna”](#) na stránce 284 to create a new certificate request that uses the key sizes you require.

Osobní certifikát má datum vypršení platnosti, po jehož uplynutí již nebude možné certifikát používat. Tato úloha vysvětluje, jak obnovit existující osobní certifikát dříve, než vyprší.

*Použití uživatelského rozhraní produktu **strmqikm***

## **Informace o této úloze**

**strmqikm** neposkytuje volbu vyhovující FIPS. Potřebujete-li spravovat certifikáty TLS způsobem, který je kompatibilní se standardem FIPS-, použijte příkaz **runmqakm**.

## **Postup**

Chcete-li požádat o osobní certifikát pomocí uživatelského rozhraní produktu **strmqikm**, proveďte následující kroky:

1. Spusťte uživatelské rozhraní pomocí příkazu **strmqikm** v systému SYSTÉM UNIX, Linuxa Okna.
2. V nabídce **Soubor databáze klíčů** klepněte na volbu **Otevřít**.  
Otevře se okno **Otevřít**.
3. Klepněte na volbu **Typ databáze klíčů** a vyberte položku **CMS** (Certificate Management System).
4. Klepněte na tlačítko **Procházet** a přejděte do adresáře, který obsahuje soubory databáze klíčů.
5. Vyberte soubor databáze klíčů, ze kterého chcete generovat požadavek, například `key.kdb`.
6. Klepněte na tlačítko **Otevřít**.  
Otevře se okno **Výzva k zadání hesla**.
7. Zadejte heslo, jež jste nastavili při vytvoření databáze klíčů, a klepněte na tlačítko **OK**.  
Název databázového souboru databáze se zobrazí v poli **Název souboru**.
8. Vyberte položku **Osobní certifikáty** z rozevírací nabídky pro výběr a vyberte certifikát ze seznamu, který chcete obnovit.
9. Klepněte na volbu **Znovu vytvořit požadavek ...** tlačítko.  
Otevře se okno, kde můžete zadat informace o názvu souboru a umístění souboru.
10. V poli **název souboru** buď přijměte výchozí hodnotu `certreq.arm`, nebo zadejte novou hodnotu včetně úplné cesty k souboru.

11. Klepněte na tlačítko **OK**. Žádost o certifikát se uloží do souboru, který jste vybrali v kroku “9” na stránce 287.
12. Vyžádejte si nový osobní certifikát odesláním souboru certifikační autoritě (CA) nebo zkopírováním souboru do formuláře požadavku na webovém serveru pro CA.

*z příkazového řádku,*

## Postup

Chcete-li požádat o osobní certifikát pomocí příkazu **runmqckm** nebo **runmqakm**, použijte následující příkazy:

- Použití produktu **runmqckm** v systémech SYSTÉM UNIX, Linuxa Okna :

```
runmqckm -certreq -recreate -db filename -pw  
password -label label  
-target filename
```

- Použití **runmqakm**:

```
runmqakm -certreq -recreate -db filename -pw  
password -label label  
-target filename
```

kde:

### **-db *název\_souboru***

Uvádí plně kvalifikovaný název souboru databáze klíčů CMS.

### **-pw *heslo***

Určuje heslo pro databázi klíčů CMS.

### **-target *název\_souboru***

Určuje název souboru pro žádost o certifikát.

## Jak pokračovat dále

Jakmile obdržíte podepsaný osobní certifikát od certifikační autority, můžete jej přidat do své databáze klíčů pomocí postupu popsaného v tématu “[Přijímání osobních certifikátů do úložiště klíčů v systému SYSTÉM UNIX, Linuxa Okna](#)” na stránce 288.

## **Přijímání osobních certifikátů do úložiště klíčů v systému SYSTÉM UNIX, Linuxa Okna**

Tento postup použijte k přijetí osobního certifikátu do souboru databáze klíčů. Úložiště klíčů musí být stejné jako úložiště, ve kterém jste vytvořili žádost o certifikát.

Poté, co vám CA pošle nový osobní certifikát, přidáte jej do souboru databáze klíčů, ze kterého jste generovali novou žádost o certifikát. Pokud CA odešle certifikát jako část e-mailové zprávy, zkopírujte tento certifikát do samostatného souboru.

## Použití produktu **strmqikm**

Potřebujete-li spravovat certifikáty TLS způsobem, který vyhovuje standardu FIPS, použijte příkaz **runmqakm**. **strmqikm** neposkytuje volbu vyhovující FIPS.

Ujistěte se, že soubor certifikátů, který má být importován, má oprávnění k zápisu pro aktuálního uživatele, a pak použijte následující proceduru buď pro správce front, nebo pro IBM MQ MQI client, aby přijal osobní certifikát do souboru databáze klíčů:

1. Spusťte grafické rozhraní pomocí příkazu **strmqikm** (na Windows SYSTÉM UNIX a 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** poté klepněte na tlačítko **OK**. Otevře se okno Výzva k zadání hesla.
7. Zadejte heslo, jež jste nastavili při vytvoření databáze klíčů, a klepněte na tlačítko **OK**. Název vašeho souboru databáze klíčů se zobrazí v poli **Název souboru**. Vyberte zobrazení **Osobní certifikáty**.
8. Klepněte na tlačítko **Přijmout**. Otevře se okno Přijmout certifikát ze souboru.
9. Zadejte název souboru certifikátu a umístění pro nový osobní certifikát, nebo klepněte na tlačítko **Procházet** a vyberte název a umístění.
10. Klepněte na tlačítko **OK**. Pokud již v databázi klíčů máte osobní certifikát, otevře se okno se žádostí, zda chcete nastavit klíč, který přidáváte jako výchozí klíč v databázi.
11. Klepněte na tlačítko **Ano** nebo **Ne**. Otevře se okno Zadat jmenovku.
12. Klepněte na tlačítko **OK**. Pole **Osobní certifikáty** zobrazuje štítek nového osobního certifikátu, který jste přidali.

## z příkazového řádku,

Chcete-li přidat osobní certifikát do souboru databáze klíčů, použijte některý z následujících příkazů:

- Použití **runmqckm**:

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

- Použití **runmqakm**:

```
runmqakm -cert -receive -file filename -db filename -pw password -fips
```

kde:

### **-file název\_souboru**

Uvádí plně kvalifikovaný název souboru osobního certifikátu.

### **-db název\_souboru**

Uvádí plně kvalifikovaný název souboru databáze klíčů CMS.

### **-pw heslo**

Určuje heslo pro databázi klíčů CMS.

### **-format ascii**

Určuje formát certifikátu. Hodnota může být `ascii` pro ASCII kódované formátem Base64 nebo `binary` pro binární data DER. Výchozí hodnota: `ascii`.

### **-fips**

určuje, že příkaz má být spuštěn v režimu FIPS. V režimu FIPS komponenta ICC používá algoritmy ověřené dle standardu FIPS 140-2. Pokud se komponenta ICC neinicializuje v režimu FIPS, příkaz **runmqakm** se nezdaří.

Používáte-li kryptografický hardware, přečtěte si téma [“Přijímání osobního certifikátu do hardwaru vašeho PKCS #11”](#) na stránce 303.

## **Extrakce certifikátu CA z úložiště klíčů v systému SYSTÉM UNIX,**

### **Linuxa Okna**

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

### **Použití produktu strmqikm**

Potřebujete-li spravovat certifikáty TLS způsobem, který vyhovuje standardu FIPS, použijte příkaz **runmqakm**. **strmqikm** (iKeyman) neposkytuje volbu vyhovující FIPS.

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

1. Spustíte grafické rozhraní pomocí příkazu **strmqikm**.
2. V nabídce **Soubor databáze klíčů** klepněte na volbu **Otevřít**. Otevře se okno Otevřít.
3. Klepněte na volbu **Typ databáze klíčů** a vyberte položku **CMS** (Certificate Management System).
4. Klepněte na tlačítko **Procházet** a přejděte do adresáře, který obsahuje soubory databáze klíčů.
5. Vyberte soubor databáze klíčů, ze kterého chcete extrahovat, například `key.kdb`.
6. Klepněte na tlačítko **Otevřít**. Otevře se okno Výzva k zadání hesla.
7. Zadejte heslo, jež jste nastavili při vytvoření databáze klíčů, a klepněte na tlačítko **OK**. Název vašeho souboru databáze klíčů se zobrazí v poli **Název souboru**.
8. V poli **Obsah databáze klíčů** vyberte **Certifikáty podepsaného** a vyberte certifikát, který chcete extrahovat.
9. Klepněte na tlačítko **Extrahovat**. Otevře se okno extrahování certifikátu do souboru.
10. Vyberte volbu **Datový typ** certifikátu, například **Base64-encoded dat ASCII** pro soubor s příponou `.arm`.
11. Zadejte název souboru certifikátu a umístění, do kterého chcete certifikát uložit, nebo klepněte na tlačítko **Procházet** a vyberte název a umístění.
12. Klepněte na tlačítko **OK**. Certifikát bude zapsán do souboru, který jste zadali.

## z příkazového řádku,

Pomocí následujících příkazů extrahujte certifikát CA pomocí **runmqckm**:

- V systému SYSTÉM UNIX, Linuxu Okna:

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

kde:

<code>-db filename</code>	je úplná cesta k databázi klíčů CMS.
<code>-pw password</code>	je heslo pro databázi klíčů CMS.
<code>-label label</code>	je jmenovka přiložená k certifikátu.
<code>-target filename</code>	je název cílového souboru.
<code>-format ascii</code>	je formát certifikátu. Hodnota může být <code>ascii</code> pro ASCII kódované formátem Base64 nebo <code>binary</code> pro binární data DER. Výchozí hodnota: <code>ascii</code> .
<code>-fips</code>	určuje, že příkaz má být spuštěn v režimu FIPS. V režimu FIPS komponenta ICC používá algoritmy ověřené dle standardu FIPS 140-2. Pokud se komponenta ICC neiniculuje v režimu FIPS, příkaz <b>runmqackm</b> se nezdaří.

## **ULW** Extrahování veřejné části certifikátu s automatickým podpisem z úložiště klíčů v systému SYSTÉM UNIX, Linuxu Okna

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

## Použití produktu **strmqikm**

Potřebujete-li spravovat certifikáty TLS způsobem, který vyhovuje standardu FIPS, použijte příkaz **runmqackm**. **strmqikm** (iKeyman) neposkytuje volbu vyhovující FIPS.



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

1. Spustíte grafické rozhraní pomocí příkazu **strmqikm** (v systému SYSTÉM UNIX, Linuxu Okna).
2. V nabídce **Soubor databáze klíčů** klepněte na volbu **Otevřít**. Otevře se okno Otevřít.
3. Klepněte na volbu **Typ databáze klíčů** a vyberte položku **CMS** (Certificate Management System).
4. Klepněte na tlačítko **Procházet** a přejděte do adresáře, který obsahuje soubory databáze klíčů.
5. Vyberte soubor databáze klíčů, ze kterého chcete extrahovat certifikát, například `key.kdb`.
6. Klepněte na tlačítko **OK**. Otevře se okno Výzva k zadání hesla.
7. Zadejte heslo, jež jste nastavili při vytvoření databáze klíčů, a klepněte na tlačítko **OK**. Název vašeho souboru databáze klíčů se zobrazí v poli **Název souboru**.
8. V poli **Obsah databáze klíčů** vyberte **Osobní certifikáty** a vyberte certifikát.
9. Klepněte na tlačítko **Extrahovat certifikát**. Otevře se okno extrahování certifikátu do souboru.
10. Vyberte volbu **Datový typ** certifikátu, například **Base64-encoded dat ASCII** pro soubor s příponou `.arm`.
11. Zadejte název souboru certifikátu a umístění, do kterého chcete certifikát uložit, nebo klepněte na tlačítko **Procházet** a vyberte název a umístění.
12. Klepněte na tlačítko **OK**. Certifikát bude zapsán do souboru, který jste zadali. Všimněte si, že když extrahujete (spíše než export) certifikát, je zahrnuta pouze veřejná část certifikátu, takže heslo není požadováno.

## z příkazového řádku,

Pomocí následujících příkazů extrahujte veřejnou část certifikátu s automatickým podpisem pomocí produktu **runmqckm** nebo **runmqakm**:

- V systému SYSTÉM UNIX, Linuxu Okna:

```
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:

<code>-db filename</code>	je úplná cesta k databázi klíčů CMS.
<code>-pw password</code>	je heslo pro databázi klíčů CMS.
<code>-label label</code>	je jmenovka přiložená k certifikátu.
<code>-target filename</code>	je název cílového souboru.
<code>-format ascii</code>	je formát certifikátu. Hodnota může být <code>ascii</code> pro ASCII kódované formátem Base64 nebo <code>binary</code> pro binární data DER. Výchozí hodnota: <code>ascii</code> .
<code>-fips</code>	určuje, že příkaz má být spuštěn v režimu FIPS. V režimu FIPS komponenta ICC používá algoritmy ověřené dle standardu FIPS 140-2. Pokud se komponenta ICC neiniculuje v režimu FIPS, příkaz <b>runmqakm</b> se nezdaří.



## Přidání certifikátu CA nebo veřejné části certifikátu podepsaného (svým držitelem) do úložiště klíčů v systému **SYSTÉM UNIX, Linuxa Okna**

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 pokračující certifikátem CA, který v řetězu bezprostředně následuje pod ním atd..

Je-li v pokynech zmíněn certifikát CA, platí tento pokyn rovněž pro veřejnou část certifikátu podepsaného (svým) držitelem.

**Poznámka:** Musíte se ujistit, že je certifikát ve formátu ASCII (UTF-8) nebo v kódování binárních (DER), protože produkt IBM Global Secure Toolkit (GSKit) nepodporuje certifikáty s jinými typy kódování.

### Použití produktu **strmqikm**

Potřebujete-li spravovat certifikáty TLS způsobem, který vyhovuje standardu FIPS, použijte příkaz **runmqakm .strmqikm** neposkytuje volbu vyhovující FIPS.

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

1. Spustíte grafické rozhraní pomocí příkazu **strmqikm** (v 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 **OK**. Otevře se okno Výzva k zadání hesla.
7. Zadejte heslo, jež jste nastavili při vytvoření databáze klíčů, a klepněte na tlačítko **OK**. Název vašeho souboru databáze klíčů se zobrazuje v poli **Název souboru**.
8. V poli **Obsah databáze klíčů** vyberte položku **Certifikáty podepsaného**.
9. Klepněte na tlačítko **Přidat**. Otevře se okno Přidat certifikát CA ze souboru.
10. Zadejte název a umístění souboru certifikátů, v němž je certifikát uložen, nebo klepněte na tlačítko **Procházet** a vyberte soubor a umístění.
11. Klepněte na tlačítko **OK**. Otevře se okno Zadat jmenovku.
12. V okně Zadat jmenovku zadejte název certifikátu.
13. Klepněte na tlačítko **OK**. Dojde k přidání certifikátu do databáze klíčů.

### z příkazového řádku,

Chcete-li přidat certifikát CA do databáze klíčů, použijte některý z následujících příkazů:

- Použití **runmqckm**:

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

- Použití **runmqakm**:

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

kde:

#### **-db název\_souboru**

Uvádí plně kvalifikovaný název souboru databáze klíčů CMS.

**-pw heslo**

Určuje heslo pro databázi klíčů CMS.

**-label popisek**

Uvádí jmenovku přiloženou k certifikátu.

**-file název\_souboru**

Uvádí jméno souboru obsahujícího certifikát.

**-format ascii**

Určuje formát certifikátu. Hodnota může být `ascii` pro ASCII kódované formátem Base64 nebo `binary` pro binární data DER. Výchozí hodnota: `ascii`.

**-fips**

určuje, že příkaz má být spuštěn v režimu FIPS. V režimu FIPS komponenta ICC používá algoritmy ověřené dle standardu FIPS 140-2. Pokud se komponenta ICC neinicializuje v režimu FIPS, příkaz `runmqkm` se nezdaří.

## **Export osobního certifikátu z úložiště klíčů v systému SYSTÉM UNIX, Linuxa Okna**

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

### **Použití produktu strmqikm**

Potřebujete-li spravovat certifikáty TLS způsobem, který vyhovuje standardu FIPS, použijte příkaz `runmqkm .strmqikm` (iKeyman) neposkytuje volbu vyhovující FIPS.

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

1. Spustíte grafické rozhraní pomocí příkazu `strmqikm` (na Windows SYSTÉM UNIX a 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,**

Chcete-li exportovat osobní certifikát pomocí produktu `runmqckm`, použijte následující příkazy:

- V systému SYSTÉM UNIX, Linuxa Okna:

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

kde:

-db <i>filename</i>	je název databáze klíčů CMS včetně cesty k souboru.
-fips	určuje, že příkaz má být spuštěn v režimu FIPS. V režimu FIPS komponenta ICC používá algoritmy ověřené dle standardu FIPS 140-2. Pokud se komponenta ICC neinicializuje v režimu FIPS, příkaz <b>runmqckm</b> se nezdaří.
-pw <i>password</i>	je heslo pro databázi klíčů CMS.
-label <i>label</i>	je jmenovka přiložená k certifikátu.
-type <i>cms</i>	je typ databáze.
-target <i>filename</i>	je úplná cesta k cílovému souboru.
-target_pw <i>password</i>	je heslo pro šifrování certifikátu.
-target_type <i>pkcs12</i>	je typ certifikátu.

## **ULW** Import osobního certifikátu do úložiště klíčů v systému SYSTÉM UNIX, Linuxa Okna

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

Před importem osobního certifikátu ve formátu PKCS #12 do souboru databáze klíčů musíte nejprve přidat celý platný řetězec certifikátu CA do souboru databáze klíčů (viz “Přidání certifikátu CA nebo veřejné části certifikátu podepsaného (svým držitelem) do úložiště klíčů v systému SYSTÉM UNIX, Linuxa Okna” na stránce 292).

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

### Použití produktu **strmqickm**

Potřebujete-li spravovat certifikáty TLS způsobem, který je kompatibilní se standardem FIPS-, použijte příkaz **runmqckm**. **strmqickm** neposkytuje volbu vyhovující FIPS.

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

1. Spustíte grafické rozhraní pomocí příkazu **strmqickm**.
2. V nabídce **Soubor databáze klíčů** klepněte na volbu **Otevřít**. Zobrazí se okno Otevřít.
3. Klepněte na volbu **Typ databáze klíčů** a vyberte položku **CMS** (Certificate Management System).
4. Klepněte na tlačítko **Procházet** a přejděte do adresáře, který obsahuje soubory databáze klíčů.
5. Vyberte soubor databáze klíčů, do nějž chcete přidat certifikát, tj. například `key.kdb`.
6. Klepněte na tlačítko **Otevřít**. Zobrazí se okno Výzva k zadání hesla.
7. Zadejte heslo, jež jste nastavili při vytvoření databáze klíčů, a klepněte na tlačítko **OK**. Název vašeho souboru databáze klíčů se zobrazuje v poli **Název souboru**.
8. V poli **Obsah databáze klíčů** vyberte **Osobní certifikáty**.
9. Pokud v zobrazení Osobní certifikáty existují certifikáty, proveďte následující kroky:
  - a. Klepněte na tlačítko **Exportovat/Importovat**. Zobrazí se okno Export/Import klíče.
  - b. Vyberte volbu **Importovat klíč**.
10. Pokud v zobrazení Osobní certifikáty nejsou žádné certifikáty, klepněte na tlačítko **Importovat**.
11. Vyberte volbu **Typ souboru s klíči** certifikátu, který chcete importovat, například PKCS12.

12. Zadejte název a umístění souboru certifikátů, v němž je certifikát uložen, nebo klepněte na tlačítko **Procházet** a vyberte soubor a umístění.
13. Klepněte na tlačítko **OK**. Zobrazí se okno Výzva k zadání hesla.
14. Do pole **Heslo** zadejte heslo, které jste použili při exportu certifikátu.
15. Klepněte na tlačítko **OK**. Zobrazí se okno Změnit popisky. Můžete změnit jmenovky importovaných certifikátů, pokud již v cílové databázi klíčů již existuje certifikát se stejným popisem. Změna návěští certifikátů nemá žádný vliv na ověření platnosti řetězu certifikátů. Chcete-li přiřadit certifikát k určitému správci front nebo IBM MQ MQI client, IBM MQ použije buď hodnotu atributu **CERTLABL**, pokud je nastavena, nebo výchozí `ibmwebspheremq` s připojeným jménem správce front nebo přihlašovacího ID uživatele IBM MQ MQI client, vše malými písmeny. Podrobnosti najdete v tématu [Digitální certifikáty certifikátu](#).
16. Chcete-li změnit popis, vyberte požadovaný popis ze seznamu **Vybrat popis, který se má změnit**. Popisek popisku se zkopíruje do vstupního pole **Zadejte nový popis**. Nahradte text popisku novým popisem a klepněte na tlačítko **Použít**.
17. Text ve vstupním poli **Zadat nový popis** bude zkopírován zpět do pole **Vybrat štítek ke změně** a nahradí původně vybraný popis 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 podepsané** s správně označenými certifikáty.
19. Certifikát je importován do databáze cílových klíčů.

## z příkazového řádku,

Chcete-li importovat osobní certifikát pomocí produktu **runmqckm**, použijte tento příkaz:

- V systému SYSTÉM UNIX, Linuxu Okna:

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

kde:

<code>-file filename</code>	je plně kvalifikovaný název souboru obsahujícího certifikát PKCS #12 .
<code>-pw password</code>	je heslo pro certifikát PKCS #12 .
<code>-type pkcs12</code>	je typ souboru.
<code>-target filename</code>	je název cílové databáze klíčů CMS.
<code>-target_pw password</code>	je heslo pro databázi klíčů CMS.
<code>-target_type cms</code>	je typ databáze určený parametrem <code>-target</code>
<code>-label label</code>	je popis certifikátu, který má být importován ze zdrojové databáze klíčů.
<code>-new_label label</code>	je popis, který bude certifikát přiřazen v cílové databázi. Vynecháte-li volbu <code>-new_label</code> , použije se výchozí hodnota pro použití stejné volby jako volba <code>-label</code> .
<code>-fips</code>	určuje, že příkaz má být spuštěn v režimu FIPS. V režimu FIPS komponenta ICC používá algoritmy ověřené dle standardu FIPS 140-2. Pokud se komponenta ICC neiniculuje v režimu FIPS, příkaz <b>runmqckm</b> se nezdaří.

Produkt **runmqckm** neposkytuje příkaz pro přímé změny popisů certifikátů. Chcete-li změnit jmenovku certifikátu, postupujte takto:

1. Exportujte certifikát do souboru PKCS #12 pomocí příkazu **-cert -export** . Uvedte 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** . Uvedte starý popis pro volbu `-label` a požadovaný nový popis pro volbu `-new_label` . Certifikát bude importován zpět do databáze klíčů s požadovaným popisem.

**ULW**

### **Importování osobního certifikátu ze souboru Microsoft.pfx**

Postupujte podle této procedury pro import ze souboru Microsoft.pfx na systému SYSTÉM UNIX, Linuxu Okna.

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 popisem 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. Spustíte grafické rozhraní pomocí příkazu **strmqikm** . Zobrazí se okno Správa klíčů IBM .
2. V nabídce **Soubor databáze klíčů** klepněte na volbu **Otevřít**. Zobrazí se okno Otevřít.
3. Vyberte typ databáze klíčů **PKCS12**.
4. **Před provedením tohoto kroku se doporučuje provést zálohování databáze pfx.** Vyberte databázi klíčů pfx, kterou chcete importovat. Klepněte na tlačítko **Otevřít**. Zobrazí se okno Výzva k zadání hesla.
5. Zadejte heslo databáze klíčů a klepněte na tlačítko **OK**. Zobrazí se okno Správa klíčů IBM . Pruh titulku zobrazuje název vybraného souboru databáze klíčů pfx označující, že soubor je otevřený a připravený.
6. Ze seznamu vyberte položku **Certifikáty podepsaného** . "Přátelské jméno" požadovaného certifikátu se zobrazí jako štítek v panelu Certifikáty podepsaného.
7. Vyberte položku štítku a klepnutím na tlačítko **Odstranit** odeberte certifikát podepsaného. Zobrazí se okno Potvrdit.
8. Klepněte na tlačítko **Ano**. Vybraný popis 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). Návrh 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:** . Nahradte text popisku popisným názvem, který byl odstraněn v kroku 7, a klepněte na tlačítko **Použít**. Popisný název musí být buď hodnota atributu IBM MQ **CERTLABL** , je-li nastaven, nebo výchozí `ibmwebsphermq` s připojeným jménem správce front nebo ID přihlášení uživatele IBM MQ MQI client , vše malými písmeny. Podrobnosti najdete v tématu [Digitální certifikáty certifikátu](#) .
21. Klepněte na tlačítko **OK**. Okno Změnit popisky je nyní odebráno a původní okno Správa klíčů produktu IBM se znovu objeví s osobními certifikáty a panely Certifikáty podepsaného, které byly aktualizovány se správně označeným osobním certifikátem.
22. Osobní certifikát pfx je nyní importován do databáze (cíle).

Není možné změnit jmenovku certifikátu pomocí **runmqckm** nebo **runmqakm**.

### **z příkazového řádku,**

Chcete-li importovat osobní certifikát pomocí produktu **runmqckm** v systému SYSTÉM UNIX, Linuxu Okna, použijte následující příkaz:

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

Chcete-li importovat osobní certifikát pomocí produktu **runmqakm**, použijte tento příkaz:

```
runmqakm -cert -import -file filename -pw password -type pkcs12 -target filename
-target_pw password -target_type cms -label label -fips -pfx
```

kde:

<code>-file filename</code>	je plně kvalifikovaný název souboru obsahujícího certifikát PKCS #12 .
<code>-pw password</code>	je heslo pro certifikát PKCS #12 .
<code>-type pkcs12</code>	je typ souboru.
<code>-target filename</code>	je název cílové databáze klíčů CMS.
<code>-target_pw password</code>	je heslo pro databázi klíčů CMS.
<code>-target_type cms</code>	je typ databáze určený parametrem <code>-target</code>
<code>-label label</code>	je popisek certifikátu, který má být importován ze zdrojové databáze klíčů.
<code>-new_label label</code>	je popisek, který bude certifikát přiřazen v cílové databázi. Vynecháte-li volbu <code>-new_label</code> , použije se výchozí hodnota pro použití stejné volby jako volba <code>-label</code> .
<code>-fips</code>	určuje, že příkaz má být spuštěn v režimu FIPS. V režimu FIPS komponenta ICC používá algoritmy ověřené dle standardu FIPS 140-2. Pokud se komponenta ICC neiniculuje v režimu FIPS, příkaz <b>runmqakm</b> se nezdaří.
<code>-pfx</code>	označuje formát souboru PFX.

Produkt **runmqckm** neposkytuje příkaz pro přímé změny popisů certifikátů. Chcete-li změnit jmenovku certifikátu, postupujte takto:

1. Exportujte certifikát do souboru PKCS #12 pomocí příkazu **-cert -export** . Uvedte 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** . Uvedte starý popisek pro volbu **-label** a požadovaný nový popisek pro volbu **-new\_label** . Certifikát bude importován zpět do databáze klíčů s požadovaným popisem.

### **ULW** Import osobního certifikátu ze souboru PKCS #7

Nástroje pro **strmqikm** (iKeyman) a **runmqckm** (iKeycmd) nepodporují PKCS #7 ( . p7b ) soubory. Použijte nástroj **runmqckm** k importu certifikátů ze souboru PKCS #7 v systému SYSTÉM UNIX, Linuxu Okna.

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

```
runmqckm -cert -add -db filename -pw password -type cms -file filename  
-label label
```

<code>-db filename</code>	je úplný název souboru databáze klíčů CMS.
<code>-pw password</code>	je heslo pro databázi klíčů.
<code>-type cms</code>	je typ databáze klíčů.
<code>-file filename</code>	je název souboru #7 PKCS.
<code>-label label</code>	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
```

<code>-db filename</code>	je plně kvalifikovaný název souboru obsahujícího certifikát PKCS #7 .
<code>-pw password</code>	je heslo pro certifikát PKCS #7 .
<code>-type pkcs7</code>	je typ souboru.
<code>-target filename</code>	je název cílové databáze klíčů.
<code>-target_pw password</code>	je heslo cílové databáze klíčů.
<code>-target_type cms</code>	je typ databáze určený parametrem <code>-target</code>
<code>-label label</code>	je jmenovka certifikátu, který má být importován.
<code>-new_label label</code>	je popisek, který bude certifikát přiřazen v cílové databázi. Vynecháte-li volbu <code>-new_label</code> , použije se výchozí hodnota pro použití stejné jako volba <code>-label</code> .

### **ULW** Odstranění certifikátu z úložiště klíčů v systému SYSTÉM UNIX, Linuxu Okna

Tento postup slouží k odebrání osobních certifikátů nebo certifikátů CA.



## Použití produktu **strmqikm**

Potřebujete-li spravovat certifikáty TLS způsobem, který vyhovuje standardu FIPS, použijte příkaz **runmqakm . strmqikm** (iKeyman) neposkytuje volbu vyhovující FIPS.

1. Spusťte grafické rozhraní pomocí příkazu **strmqikm** (v systému SYSTÉM UNIX, Linuxa Okna).
2. V nabídce **Soubor databáze klíčů** klepněte na volbu **Otevřít**. Otevře se okno Otevřít.
3. Klepněte na volbu **Typ databáze klíčů** a vyberte položku **CMS** (Certificate Management System).
4. Klepněte na tlačítko **Procházet** a přejděte do adresáře, který obsahuje soubory databáze klíčů.
5. Vyberte soubor databáze klíčů, ze kterého chcete odstranit certifikát, například `key .kdb`.
6. Klepněte na tlačítko **Otevřít**. Otevře se okno Výzva k zadání hesla.
7. Zadejte heslo, jež jste nastavili při vytvoření databáze klíčů, a klepněte na tlačítko **OK**. Název vašeho souboru databáze klíčů se zobrazí v poli **Název souboru**.
8. Z rozevíracího seznamu vyberte **Osobní certifikáty** nebo **Certifikáty podepsaného**
9. Vyberte certifikát, který chcete odstranit.
10. Pokud ještě nemáte kopii certifikátu a chcete ji uložit, klepněte na volbu **Exportovat/Importovat** a exportujte ji (viz “Export osobního certifikátu z úložiště klíčů v systému SYSTÉM UNIX, Linuxa Okna” na stránce 293).
11. S vybraným certifikátem klepněte na tlačítko **Odstranit**. Otevře se okno Potvrdit.
12. Klepněte na tlačítko **Ano**. Pole **Osobní certifikáty** již nezobrazuje štítek certifikátu, který jste odstranili.

## z příkazového řádku,

Pomocí následujících příkazů odstraníte certifikát pomocí **runmqckm**:

- V systému SYSTÉM UNIX, Linuxa Okna:

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

kde:

-db <i>filename</i>	je plně kvalifikovaný název souboru databáze klíčů CMS.
-pw <i>password</i>	je heslo pro databázi klíčů CMS.
-label <i>label</i>	je jmenovka přiložená k osobnímu certifikátu.
-fips	určuje, že příkaz má být spuštěn v režimu FIPS. V režimu FIPS komponenta ICC používá algoritmy ověřené dle standardu FIPS 140-2. Pokud se komponenta ICC neiniculuje v režimu FIPS, příkaz <b>runmqakm</b> se nezdaří.

## **ULW** Generování silných hesel pro ochranu úložiště klíčů v systému SYSTÉM UNIX, Linuxa Okna

Pomocí příkazu **runmqakm** (GSKCapiCmd) můžete generovat silná hesla pro ochranu pomocí úložiště klíčů.

Chcete-li vygenerovat silné heslo, můžete použít příkaz **runmqakm** s následujícími parametry:

```
runmqakm -random -create -length 14 -strong -fips
```



Při použití vygenerovaného hesla v parametru **-pw** v následujících příkazech pro administraci certifikátů vždy uzavřete heslo do dvojitých uvozovek. Na systémech SYSTÉM UNIX a Linux musíte také použít znak zpětného lomítka, abyste se vyhnuli následujícím znakům, pokud se objeví v řetězci hesla:

```
! \ " ' `
```

Při zadávání hesla v odezvě na výzvu z produktu **runmqckm**, **runmqakm** nebo GUI **strmqikm** není nutné, aby heslo ucitli nebo aby se z něj vytekli. Není to nutné, protože shell operačního systému nemá vliv na zadávání dat v těchto případech.

### **Konfigurace pro kryptografický hardware na systémech UNIX, Linux nebo Windows**

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

Šifrovací hardware pro správce front lze konfigurovat pro systémy 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 nástroj IBM MQ Explorer ke konfiguraci kryptografického hardwaru na systému UNIX, Linux nebo Windows . Další informace najdete v online nápovědě.

You can configure cryptographic hardware for an IBM MQ client on UNIX, Linux or Windows systems using either of the following methods:

- Nastavte proměnnou prostředí MQSSLCRYP. Povolené hodnoty pro vlastnost MQSSLCRYP jsou stejné jako u parametru SSLCRYP, jak je popsáno v tématu [ALTER QMGR](#).

Pokud použijete verzi parametru SSLCRYP GSK\_PKCS11 , štítek tokenu PKCS #11 se musí shodovat s popisem, se kterým jste nakonfigurovali hardware.

- 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. Tento popis je popsán v tématu [“Správa certifikátů na hardwaru PKCS #11”](#) na stránce 300.

#### **ULW**

#### *Správa certifikátů na hardwaru PKCS #11*

Můžete spravovat digitální certifikáty na kryptografickém hardwaru, který podporuje rozhraní PKCS #11 .

### **Informace o této úloze**

Musíte vytvořit databázi klíčů pro přípravu prostředí produktu IBM MQ , a to i v případě, že nechcete v něm ukládat certifikáty certifikační autority (CA), ale budou ukládat všechny své certifikáty na váš kryptografický hardware. Databáze klíčů je nezbytná, aby správce front odkazoval na své pole SSLKEYR nebo pro aplikaci klienta na odkaz v proměnné prostředí MQSSLKEYR. Tato databáze klíčů je také povinná, pokud vytváříte žádost o certifikát.

Databázi klíčů vytvoříte buď pomocí příkazového řádku, nebo pomocí uživatelského rozhraní produktu **strmqikm** (iKeyman).

### **Postup**

Vytvořte databázi klíčů pomocí příkazového řádku.

1. Spusťte některý z následujících příkazů:

- Použití **runmqckm**:

```
runmqckm -keydb -create -db filename -pw password -type cms -stash
```

- Použití **runmqakm**:

```
runmqakm -keydb -create -db filename -pw password -type cms
-stash -fips -strong
```

kde:

**-db název\_souboru**

Uvádí plně kvalifikovaný název souboru databáze klíčů CMS a musí mít příponu souboru .kdb.

**-pw heslo**

Určuje heslo pro databázi klíčů CMS.

**-type cms**

Uvádí typ databáze. (Pro IBM MQ musí být cms.)

**-stash**

Uloží heslo databáze klíčů do souboru.

**-fips**

určuje, že příkaz má být spuštěn v režimu FIPS. Při použití režimu FIPS komponenta ICC používá algoritmy, které jsou validovány FIPS 140-2. Pokud se komponenta ICC neiniculuje v režimu FIPS, příkaz **runmqakm** se nezdaří.

**-silné**

Kontroluje, zda zadané heslo splňuje minimální požadavky na odolnost hesla. Minimální požadavky na heslo jsou tyto:

- Heslo musí mít minimální délku 14 znaků.
- Heslo musí obsahovat minimálně jedno malé písmeno, jedno velké písmeno a jednu číslici nebo speciální znak. Mezi speciální znaky patří hvězdička (\*), znak dolaru (\$), symbol čísla (#) a znak procenta (%). Prostor je klasifikován jako speciální znak.
- Každý znak může v hesle nastat maximálně třikrát.
- Maximální počet dvou po sobě jdoucích znaků v hesle může být stejný.
- Všechny znaky jsou ve standardním tisknutelném znakové sadě ASCII, v rozsahu 0x20 - 0x7E.

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

2. V systémech SYSTÉM UNIX a Linux se přihlaste jako uživatel root. V systému Windows se přihlaste jako administrátor nebo jako člen skupiny MQM.
3. Otevřete soubor vlastností zabezpečení Java, `java.security`.

- Na systémech SYSTÉM UNIX a Linux je soubor vlastností zabezpečení Java umístěn v podadresáři `java/jre64/jre/lib/security` instalačního adresáře produktu IBM MQ.
- Na systémech Windows je soubor vlastností zabezpečení Java umístěn v podadresáři `java\jre\lib\security` instalačního adresáře produktu IBM MQ.

Pokud se v souboru dosud nenachází, přidejte poskytovatele zabezpečení `IBMPKCS11Impl`. Například přidáním následujícího řádku:

```
security.provider.12=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl
```

4. Spusťte uživatelské rozhraní spuštěním příkazu **strmqikm**.
5. Klepněte na nabídku **Soubor databáze klíčů > Otevřít**.
6. Klepněte na volbu **Typ databáze klíčů** a vyberte volbu **PKCS11Direct**.
7. Do pole **Název souboru** zadejte název modulu správy kryptografického hardwaru, například `PKCS11_API.so`.

Používáte-li certifikáty nebo klíče uložené na šifrovacím hardwaru PKCS #11, uvědomte si, že 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, neboť programy iKeyman a iKeycmd jsou na těchto platformách 32bitové.

8. Do pole **Umístění** zadejte cestu:

- V systémech SYSTÉM UNIX a Linux to může být například /usr/lib/pkcs11.
- V systému Windows můžete zadat název knihovny, například cryptoki.

Klepněte na tlačítko **OK**. Otevře se okno Otevřít kryptografický token.

9. Vyberte popisek tokenu šifrovacího zařízení, který chcete použít k ukládání certifikátů.

10. Do pole **Heslo šifrovacího tokenu** zadejte heslo, které jste nastavili při konfiguraci kryptografického hardwaru.

11. Má-li váš kryptografický hardware kapacitu k ukládání certifikátů podepisujících subjektů požadovaných pro příjem nebo import osobního certifikátu, zrušte zaškrtnutí obou políček sekundární databáze klíčů a pokračujte krokem “15” na stránce 302.

Pokud vyžadujete, aby sekundární databáze klíčů CMS byla držitelem certifikátů podepsaného, vyberte buď volbu **Otevřít existující soubor databáze sekundárních klíčů** , nebo volbu **Vytvořit nový soubor databáze sekundárního klíče**.

12. Do pole **Název souboru** zadejte název souboru. Toto pole již obsahuje text key . kdb. Pokud je váš název kmene key, ponechte toto pole nezměněné. Pokud jste uvedli jiný název souboru, nahraďte key svým kmenovým jménem. Nesmíte změnit příponu . kdb .

13. V poli **Umístění** zadejte cestu, například:

- Pro správce front: /var/mqm/qmgrs/QM1/ssl
- Pro IBM MQ MQI client: /var/mqm/ssl

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

14. Zadejte heslo.

Pokud jste v kroku “11” na stránce 302 vybrali volbu **Otevřít existující databázový soubor sekundárního klíče** , zadejte do pole **Heslo** heslo.

Pokud jste v kroku “11” na stránce 302 vybrali volbu **Vytvořit nový soubor databáze sekundárního klíče** , proveďte následující dílčí kroky:

- a) Do pole **Heslo** zadejte heslo a zadejte je znovu do pole **Potvrdit heslo** .
- b) Vyberte **Stash heslo pro soubor**. Všimněte si, že pokud heslo nezamačujete, pokusy o spuštění kanálů TLS selžou, protože nemohou získat heslo požadované pro přístup k souboru databáze klíčů.
- c) Klepněte na tlačítko **OK**. Otevře se okno s potvrzením, že heslo je v souboru key . sth (pokud jste neuvedli jiný název kmene).

15. Klepněte na tlačítko **OK**. Zobrazí se rámec s informacemi o obsahu databáze klíčů.

#### Požádání o osobní certifikát pro hardware PKCS #11

Tento postup použijte buď pro správce front, nebo pro IBM MQ MQI client , abyste požádali o osobní certifikát pro váš kryptografický hardware.

### Informace o této úloze

Tato úloha popisuje, jak používat uživatelské rozhraní produktu **strmqikm** k vyžádání osobního certifikátu. Pokud používáte rozhraní příkazového řádku, prohlédněte si téma “[z příkazového řádku](#),” na stránce 285.

**Poznámka:** Produkt IBM MQ nepodporuje algoritmy SHA-3 nebo SHA-5 . Můžete použít názvy algoritmů digitálního podpisu SHA384WithRSA a SHA512WithRSA , protože oba algoritmy jsou členy řady SHA-2 .

Názvy algoritmů digitálního podpisu SHA3WithRSA a SHA5WithRSA jsou zamítnuty, protože se jedná o zkrácený tvar SHA384WithRSA a SHA512WithRSA .

## Postup

Chcete-li požádat o osobní certifikát z uživatelského rozhraní produktu **strmqikm** (iKeyman), postupujte takto:

1. Postupujte takto, abyste mohli pracovat s vaším kryptografickým hardwarem. Viz [“Správa certifikátů na hardwaru PKCS #11”](#) na stránce 300.
2. V nabídce **Vytvořit** klepněte na **Nový požadavek na certifikát**.  
Otevře se okno Vytvořit nový klíč a žádost o certifikát.
3. Do pole **Jmenovka klíče** zadejte jmenovku certifikátu.  
Jmenovka je buď hodnota atributu **CERTLABL**, je-li nastavena, nebo standardní **ibmwebspheremq** s připojeným jménem správce front nebo IBM MQ MQI client ID uživatele pro přihlášení, vše malými písmeny. Podrobnosti najdete v tématu [Digitální certifikáty certifikátu](#).
4. Vyberte volbu **Velikost klíče** a **Algoritmus podpisu**, které požadujete.
5. Zadejte hodnoty do pole **Obecný název** a **Organizace** a vyberte volbu **Země**. U zbývajících volitelných polí buď přijměte výchozí hodnoty, nebo zadejte nové hodnoty nebo vyberte nové hodnoty.  
Všimněte si, že v poli **Organizační jednotka** můžete zadat pouze jeden název. Další informace o těchto polích naleznete v tématu [“Rozlišující názvy”](#) na stránce 11.
6. Do pole **Zadejte název souboru, do kterého chcete uložit žádost o certifikát**, buď přijměte výchozí **certreq.arm**, nebo zadejte novou hodnotu s úplnou cestou.
7. Klepněte na tlačítko **OK**.  
Otevře se okno Potvrzení.
8. Klepněte na tlačítko **OK**.  
V seznamu **Požadavky na osobní certifikáty** je zobrazen popis nové žádosti o osobní certifikát, kterou jste vytvořili. Požadavek na certifikát je uložen v souboru, který jste zvolili v kroku [“6”](#) na stránce 303.
9. Vyžádejte si nový osobní certifikát odesláním souboru certifikační autoritě (CA) nebo zkopírováním souboru do formuláře požadavku na webovém serveru pro CA.

### *Přijímání osobního certifikátu do hardwaru vašeho PKCS #11*

Tento postup použijte buď pro správce front, nebo pro produkt IBM MQ MQI client, který obdrží osobní certifikát pro váš kryptografický hardware.

## Než začnete

Přidejte certifikát CA od CA, který podepsal osobní certifikát. Přidejte ji buď do kryptografického hardwaru, nebo do sekundární databáze klíčů CMS. Tuto akci proveďte před tím, než obdržíte podepsaný certifikát do kryptografického hardwaru. Chcete-li přidat certifikát CA do svazku klíčů, postupujte podle pokynů v části [“Přidání certifikátu CA nebo veřejné části certifikátu podepsaného \(svým držitelem\) do úložiště klíčů v systému SYSTÉM UNIX, Linuxu Okna”](#) na stránce 292.

## Procedura

- Chcete-li obdržet osobní certifikát pomocí uživatelského rozhraní produktu **strmqikm** (iKeyman), postupujte takto:
  - a) Postupujte takto, abyste mohli pracovat s vaším kryptografickým hardwarem. Viz [“Správa certifikátů na hardwaru PKCS #11”](#) na stránce 300.
  - b) Klepněte na tlačítko **Přijmout**. Otevře se okno Přijmout certifikát ze souboru.
  - c) Zadejte název souboru certifikátu a umístění pro nový osobní certifikát, nebo klepněte na tlačítko **Procházet** a vyberte název a umístění.
  - d) Klepněte na tlačítko **OK**. Pokud již v databázi klíčů máte osobní certifikát, otevře se okno s dotazem, zda chcete nastavit klíč, který přidáváte jako výchozí klíč v databázi.
  - e) Klepněte na tlačítko **Ano** nebo **Ne**. Otevře se okno Zadat jmenovku.

- f) Klepněte na tlačítko **OK**. V seznamu **Osobní certifikáty** je zobrazen popis nového osobního certifikátu, který jste přidali. Tento štítek je vytvořen přidáním štítku šifrovacího tokenu před popis, který jste zadali.
- Chcete-li obdržet osobní certifikát pomocí příkazu **runmqakm** (GSKCapiCmd), proveďte následující kroky:
    - a) Otevřete příkazové okno, které je nakonfigurované pro vaše prostředí.
    - b) Přijmout osobní certifikát pomocí příkazu **runmqakm** (GSKCapiCmd):

```
runmqakm -cert -receive -file filename -crypto module_name
         -tokenlabel hardware_token -pw hardware_password
         -format cert_format -fips
         -secondaryDB filename -secondaryDBpw password
```

kde:

**-file *název\_souboru***

Uvádí plně kvalifikovaný název souboru, který obsahuje osobní certifikát.

**-šifrování *název\_modulu***

Uvádí plně kvalifikovaný název knihovny PKCS #11 dodané s kryptografickým hardwarem.

**-tokenlabel *hardwareční\_token***

Uvádí jmenovku tokenu šifrovacího zařízení PKCS #11 .

**-pw *heslo\_hardwaru\_hardwaru***

Určuje heslo pro přístup k kryptografickému hardwaru.

**-format *formát\_certifikátu***

Určuje formát certifikátu. Hodnota může být `ascii` pro ASCII kódované formátem Base64 nebo `binary` pro binární data DER. Předvolba je ASCII.

**-fips**

určuje, že příkaz má být spuštěn v režimu FIPS. Při použití režimu FIPS komponenta ICC používá algoritmy, které jsou validovány FIPS 140-2. Pokud se komponenta ICC neiniculuje v režimu FIPS, příkaz **runmqakm** se nezdaří.

**-secondaryDB *název\_souboru***

Uvádí plně kvalifikovaný název souboru databáze klíčů CMS.

**-secondaryDBpw *heslo***

Určuje heslo pro databázi klíčů CMS.

## Práce s TLS v systému IBM MQ Appliance

IBM MQ Appliance má podporu TLS (Transport Layer Security).

IBM MQ Appliance má odlišné příkazy pro správu certifikátů. Podrobné informace o správě certifikátů viz dokumentace produktu IBM MQ Appliance , [správa certifikátů TLS](#) .

## Práce s SSL nebo TLS v systému z/OS

Tyto informace popisují, jak jste nastavili a pracují se zabezpečením SSL (Secure Sockets Layer) nebo TLS (Transport Layer Security) na serveru z/OS.

Každé téma obsahuje příklady provedení jednotlivých úloh pomocí produktu RACF. Podobné úlohy můžete provádět pomocí jiných externích správců zabezpečení.

V systému z/OS je třeba nastavit také počet dílčích úloh serveru, které každý správce front používá pro zpracování volání SSL, jak je popsáno v tématu [“Nastavení parametru SSLTASKS”](#) na stránce 305.

z/OS Podpora SSL je integrální součástí operačního systému a je známá jako *System SSL*. System SSL je součástí základního prvku Cryptographic Services Base produktu z/OS. Základní členové produktu Cryptographic Services Base jsou nainstalováni v adresáři *pdsname*. Sada datových sad SEIALNKE (rozdělená datová sada (PDS)). Při instalaci zabezpečení SSL systému se ujistěte, že jste zvolili příslušné volby pro poskytnutí vámi vyžadování CipherSpecs .

## Další požadavky na ID uživatele

Tyto informace popisují další požadavky, které vaše ID uživatele potřebuje pro nastavení a práci s TLS nebo SSL na systému z/OS.

Ujistěte se, že máte ve svém systému všechny vhodné aktualizace typu High Impact nebo Pervasive (HIPER).

Ujistěte se, že jste nastavili následující předpoklady:

- ID uživatele *ssidCHIN* je v produktu RACFsprávně definováno a že ID uživatele *ssidCHIN* má přístup pro čtení k následujícím profilům:
  - IRR.DIGTCERT.LIST
  - IRR.DIGTCERT.LISTRING

Tyto proměnné jsou definovány ve třídě FACILITY RACF .

- ID uživatele *ssidCHIN* je vlastníkem svazku klíčů.
- Osobní certifikát správce front, pokud byl vytvořen příkazem RACDCERT, je vytvořen s ID uživatele pro typ certifikátu, který je také stejný jako ID uživatele *ssidCHIN* .
- Inicializátor kanálu je recyklován nebo je zadán příkaz **REFRESH SECURITY TYPE(SSL)** k výběru všech změn, které jste provedli v klíčovém kruhu.
- Procedura iniciátoru kanálu produktu IBM MQ má přístup k systémové knihovně běhového prostředí SSL *název\_dsn*.SIEALNIKE prostřednictvím seznamu odkazů, LPA nebo příkazu STEPLIB DD. Tato knihovna musí být autorizovaná APF.
- ID uživatele, pod jehož oprávněním je spuštěn inicializátor kanálu, je nakonfigurováno pro použití služeb systému UNIX System Services (USS), jak je popsáno v dokumentaci k produktu z/OS UNIX System Services Planning.

Uživatelé, kteří nechtějí, aby iniciátor kanálu vyvolali systémové služby UNIX s použitím *guest/default* UID a segmentu OMVS, potřebuje pouze modelovat nový segment OMVS na základě výchozího segmentu, protože iniciátor kanálu nevyžaduje žádná speciální oprávnění a nespouští se v rámci UNIX jako superuživatel.

### Nastavení parametru SSLTASKS

Pomocí příkazu ALTER QMGR nastavte počet podúloh serveru pro zpracování volání SSL.

Chcete-li používat kanály zabezpečení SSL, zajistěte, aby při nastavení parametru SSLTASKS byl použit parametr SSLTASKS s alespoň dvěma podúlohami serveru, pomocí příkazu ALTER QMGR. Příklad:

```
ALTER QMGR SSLTASKS(5)
```

Chcete-li se vyhnout problémům s přidělením úložiště, nenastavujte atribut SSLTASKS na hodnotu větší než osm v prostředí, kde není kontrolována seznam CRL (Certificate Revocation List).

Je-li použita kontrola CRL, je v daném kanálu zadržen SSLTASK po dobu trvání této kontroly. Důvodem může být významná uplynulá doba, kdy je kontaktován relevantní server LDAP, protože každá SSLTASK je řídicí blok úloh z/OS .

Chcete-li změnit hodnotu atributu SSLTASKS, musíte restartovat inicializátor kanálu.

### Nastavení úložiště klíčů v systému z/OS

Nastavte úložiště klíčů na obou koncích připojení. Přidruzte každé úložiště klíčů ke svému správci front.

Připojení SSL nebo TLS vyžaduje *úložiště klíčů* na každém konci připojení. Každý správce front musí mít přístup k úložišti klíčů. Chcete-li přiřadit úložiště klíčů ke správci front, použijte parametr SSLKEYR v příkazu ALTER QMGR. Další informace viz [“Úložiště klíčů SSL nebo TLS”](#) na stránce 23.

V operačním systému z/OS jsou digitální certifikáty uloženy v *svazku klíčů* spravovaném externím správcem zabezpečení (ESM). Tyto digitální certifikáty mají štítky, které přidružují certifikát ke správci

front. SSL a TLS používají tyto certifikáty pro účely autentizace. Všechny příklady, které následují za použití příkazů RACF . Pro ostatní programy ESM existují ekvivalentní příkazy.

V systému z/OS používá produkt IBM MQ buď hodnotu atributu **CERTLABL** , pokud je nastavena, nebo výchozí `ibmWebSphereMQ` s připojeným názvem správce front. Podrobnosti najdete v tématu [Digitální certifikáty certifikátu](#) .

Název úložiště klíčů pro správce front je názvem svazku klíčů ve vaší databázi RACF . Název klíčového řetězce můžete zadat buď před nebo po vytvoření svazku klíčů.

Chcete-li vytvořit nový svazek klíčů pro správce front, postupujte takto:

1. Ujistěte se, že máte odpovídající oprávnění pro vydání příkazu RACDCERT (viz *SecureWay Security Server RACF Command Language Reference* , kde získáte další podrobnosti).
2. Spusťte následující příkaz:

```
RACDCERT ID( userid1 ) ADDRING( ring-name )
```

kde:

- *userid1* je ID uživatele adresního prostoru inicializátoru kanálu nebo ID uživatele, které bude vlastnit klíč svazku klíčů (je-li svazek klíčů sdílený).
- *ring-name* je jméno, které chcete dát do svazku klíčů. Délka tohoto názvu může být až 237 znaků. V tomto jménu se rozlišují velká a malá písmena. Chcete-li se vyhnout problémům, zadejte velkými písmeny řetězec *ring-name* .

*Zpřístupnění certifikátů CA pro správce front v systému z/OS*

Po vytvoření svazku klíčů připojte k němu všechny příslušné certifikáty CA.

Máte-li v datové sadě certifikát CA, musíte nejprve přidat certifikát do databáze RACF® pomocí následujícího příkazu:

```
RACDCERT ID( userid1 ) ADD( input-data-set-name ) WITHLABEL( 'My CA' )
```

Poté pro připojení certifikátu CA pro `My CA` ke svému svazku klíčů použijte tento příkaz:

```
RACDCERT ID(userid1)  
CONNECT(CERTAUTH LABEL('My CA') RING(ring-name) USAGE(CERTAUTH))
```

kde *userid1* je buď ID uživatele iniciátoru kanálu, nebo vlastník sdíleného svazku klíčů.

Další informace o certifikátech CA najdete v tématu [“digitální certifikáty”](#) na stránce 9.

### **Vyhledání úložiště klíčů pro správce front v systému z/OS**

Tuto proceduru použijte k získání umístění svazku klíčů správce front.

1. Zobrazte atributy správce front pomocí jednoho z následujících příkazů MQSC:

```
DISPLAY QMGR ALL  
DISPLAY QMGR SSLKEYR
```

2. Prohlédněte si výstup příkazu pro umístění svazku klíčů.

### **Určení umístění úložiště klíčů pro správce front**

Chcete-li zadat umístění svazku klíčů správce front, nastavte atribut úložiště klíčů správce front pomocí příkazu ALTER QMGR MQSC.

Příklad:

```
ALTER QMGR SSLKEYR(CSQ1RING)
```



pokud je svazek klíčů vlastněný adresním prostorem inicializátoru kanálu, nebo:

```
ALTER QMGR SSLKEYR(userid1/CSQ1RING)
```

pokud se jedná o sdílený svazek klíčů, kde *userid1* je ID uživatele, který vlastní tento svazek klíčů.

### **Poskytnutí správných přístupových práv inicializátoru kanálu**

Inicializátor kanálu (CHINIT) potřebuje přístup k úložišti klíčů a k určitým profilům zabezpečení.

### **Udělení přístupu CHINIT ke čtení úložiště klíčů**

Je-li úložiště klíčů vlastněno ID uživatele CHINIT, tento ID uživatele potřebuje přístup pro čtení k IRR.DIGTCERT.LISTRING profilu ve třídě FACILITY a v opačném případě aktualizujte přístup. Udělte přístup pomocí příkazu PERMIT s možností ACCESS (UPDATE) nebo ACCESS (READ) podle potřeby:

```
PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID( userid ) ACCESS(UPDATE)
```

kde *id\_uživatele* je ID uživatele adresního prostoru inicializátoru kanálu.

### **Udělení přístupu pro čtení CHINIT k příslušným profilům CSF\***

Pro použití hardwarové podpory poskytované prostřednictvím rozhraní ICSF (Integrated Cryptographic Service Facility) zajistěte, aby vaše ID uživatele CHINIT mělo přístup pro čtení k příslušným profilům CSF\* ve třídě CSFSERV pomocí následujícího příkazu:

```
PERMIT csf-resource CLASS(CSFSERV) ID( userid ) ACCESS(READ)
```

kde *csf-resource* je název profilu CSF\* a *userid* je ID uživatele adresního prostoru inicializátoru kanálu.

Zopakujte tento příkaz pro každý z následujících názvů profilů CSF\*:

- CSFPKD
- CSFPKE
- CSFPKI
- CSFDSG
- CSFDSV

Pokud jsou vaše klíče certifikátů uloženy ve službě ICSF a vaše instalace zavedla řízení přístupu přes klíče uložené v ICSF, ujistěte se, že vaše ID uživatele CHINIT má přístup pro čtení k profilu ve třídě CSFKEYS pomocí následujícího příkazu:

```
PERMIT IRR.DIGTCERT. userid.* CLASS(CSFKEYS) ID( userid ) ACCESS(READ)
```

kde *id\_uživatele* je ID uživatele adresního prostoru inicializátoru kanálu.

### **Použití programu ICSF (Integrated Cryptographic Service Facility)**

Inicializátor kanálu může použít službu ICSF k vygenerování náhodného čísla při zavedení algoritmu ochrany heslem pro zamaskování hesel procházejících přes kanály klienta, pokud se nepoužívá SSL/TLS.

Další informace naleznete v tématu [“Použití programu ICSF \(Integrated Cryptographic Service Facility\)”](#) na stránce 246 .

### **Když změny certifikátů nebo úložiště klíčů vstoupí v platnost v z/OS**

Změny se projeví po spuštění inicializátoru kanálu nebo při aktualizaci úložiště.



Konkrétně změny certifikátů v souboru svazku klíčů a atributu úložiště klíčů se projeví při jedné z následujících akcí:

- Při spuštění nebo restartování inicializátoru kanálu.
- Když je vydán příkaz REFRESH SECURITY TYPE (SSL) k obnovení obsahu úložiště klíčů SSL.

### **Vytvoření osobního certifikátu podepsaného sebou samým na serveru z/OS**

Pomocí této procedury vytvoříte osobní certifikát podepsaný sám sebou samým.

1. Vygenerujte certifikát a dvojici veřejného a soukromého klíče pomocí následujícího příkazu:

```
RACDCERT ID(userid2) GENCERT
SUBJECTSDN(CN('common-name')
            T('title')
            OU('organizational-unit')
            O('organization')
            L('locality')
            SP('state-or-province')
            C('country'))
WITHLABEL('label-name')
```

2. Připojte certifikát ke svému svazku klíčů pomocí následujícího příkazu:

```
RACDCERT ID(userid1)
CONNECT(ID(userid2) LABEL('label-name') RING(ring-name) USAGE(PERSONAL))
```

kde:

- *userid1* je ID uživatele adresního prostoru inicializátoru kanálu nebo vlastník sdíleného svazku klíčů.
- *userid2* je ID uživatele přidružené k certifikátu a musí se jednat o ID uživatele adresního prostoru inicializátoru kanálu.

*userid1* a *userid2* mohou být stejné ID.

- Parametr *název-svazku* je název, který jste přiřadili svazku klíčů v produktu [“Nastavení úložiště klíčů v systému z/OS”](#) na stránce 305.
- *název-návěští* musí být buď hodnota atributu IBM MQ **CERTLABL**, je-li nastavena, nebo výchozí `ibmWebSphereMQ` s připojeným názvem správce front. Podrobnosti najdete v tématu [Digitální certifikáty certifikátu](#).

### **Požádání o osobní certifikát v systému z/OS**

Použijte pro osobní certifikát pomocí produktu RACF.

Chcete-li požádat o osobní certifikát, použijte příkaz RACF takto:

1. Vytvořte osobní certifikát podepsaný sám sebou, jako v produktu [“Vytvoření osobního certifikátu podepsaného sebou samým na serveru z/OS”](#) na stránce 308. Tento certifikát poskytuje požadavek s hodnotami atributu pro rozlišující název.
2. Vytvořte požadavek certifikátu PKCS #10 Base64-encoded napsaný do datové sady pomocí následujícího příkazu:

```
RACDCERT ID(userid2) GENREQ(LABEL('label_name ')) DSN('output_data_set_name')
```

kde:

- *userid2* je ID uživatele přidružené k certifikátu a musí to být ID uživatele adresního prostoru inicializátoru kanálu
- *label\_name* je jmenovka použitá při vytváření certifikátu podepsaného sebou samým

Podrobnosti viz [“Digitální certifikáty certifikátu, základní informace o požadavcích”](#) na stránce 25.

3. Chcete-li požádat o nový osobní certifikát, odešlete datovou sadu certifikační autoritě (CA).

4. Když je podepsaný certifikát vrácen certifikační autoritou, přidejte certifikát zpět do databáze RACF pomocí původní jmenovky, jak je popsáno v [“Přidání osobních certifikátů do úložiště klíčů v systému z/OS”](#) na stránce 309.

### **Vytvoření osobního certifikátu podepsaného RACF**

Produkt RACF může fungovat jako certifikační autorita a vydává svůj vlastní certifikát CA.

Tento oddíl používá termín *certifikát podepisujícího subjektu* k označení certifikátu CA vydaného produktem RACF.

Soukromý klíč pro certifikát podepsaného musí být v databázi RACF před tím, než provedete následující proceduru:

1. Pomocí následujícího příkazu vygenerujte osobní certifikát podepsaný pomocí produktu RACFs použitím certifikátu podepsaného obsaženého ve vaší databázi RACF :

```
RACDCERT ID(userid2) GENCERT
SUBJECTSDN(CN('common-name')
            T('title')
            OU('organizational-unit')
            O('organization')
            L('locality')
            SP('state-or-province')
            C('country'))
WITHLABEL('label-name')
SIGNWITH(CERTAUTH LABEL('signer-label'))
```

2. Připojte certifikát ke svému svazku klíčů pomocí následujícího příkazu:

```
RACDCERT ID(userid1)
CONNECT(ID(userid2) LABEL('label-name') RING(ring-name) USAGE(PERSONAL))
```

kde:

- *userid1* je ID uživatele adresního prostoru inicializátoru kanálu nebo vlastník sdíleného svazku klíčů.
- *userid2* je ID uživatele přidružené k certifikátu a musí se jednat o ID uživatele adresního prostoru inicializátoru kanálu.  
*userid1* a *userid2* mohou být stejné ID.
- Parametr *název-svazku* je název, který jste přiřadili svazku klíčů v produktu [“Nastavení úložiště klíčů v systému z/OS”](#) na stránce 305.
- Hodnota *název-návěští* musí být buď hodnota atributu IBM MQ **CERTLABL** , je-li nastavena, nebo výchozí `ibmWebSphereMQ` s připojeným názvem správce front nebo skupiny sdílení front. Podrobnosti najdete v tématu [Digitální certifikáty certifikátu](#) .
- *signer-label* je popisek vašeho vlastního certifikátu podepisujícího subjektu.

### **Přidání osobních certifikátů do úložiště klíčů v systému z/OS**

Tento postup slouží k přidání nebo importu osobního certifikátu do svazku klíčů.

Poté, co vám certifikační autorita odešle nový osobní certifikát, přidejte jej do svazku klíčů pomocí následující procedury:

1. Přidejte certifikát do databáze produktu RACF pomocí následujícího příkazu:

```
RACDCERT ID( userid2 ) ADD( input-data-set-name ) WITHLABEL(' label-name ')
```

2. Připojte certifikát ke svému svazku klíčů pomocí následujícího příkazu:

```
RACDCERT ID( userid1 )
CONNECT(ID( userid2 ) LABEL(' label-name ') RING( ring-name ) USAGE(PERSONAL))
```

kde:

- *userid1* je ID uživatele adresního prostoru inicializátoru kanálu nebo vlastník sdíleného svazku klíčů.
- *userid2* je ID uživatele přidružené k certifikátu a musí se jednat o ID uživatele adresního prostoru inicializátoru kanálu.
- Parametr *název-svazku* je název, který jste přiřadili svazku klíčů v produktu “Nastavení úložiště klíčů v systému z/OS” na stránce 305.
- *název-vstupní-datové-sady* je název datové sady, která obsahuje podepsaný certifikát CA. Datová sada musí být katalogizována a nesmí se jednat o rozdělenou datovou sadu (PDS) nebo o člen rozdělené datové sady (PDS). Formát záznamu (RECFM), který očekává RACDCERT, je VB. RACDCERT dynamicky přiděluje a otevře datovou sadu a přečte certifikát z něj jako binární data.
- *název-popisku* je název popisku, který byl použit při vytvoření původní žádosti. Musí to být buď hodnota atributu IBM MQ **CERTLABL**, je-li nastavena, nebo výchozí *ibmWebSphereMQ* s připojeným názvem správce front nebo skupiny sdílení front. Podrobnosti najdete v tématu [Digitální certifikáty certifikátu](#).

### **Export osobního certifikátu z úložiště klíčů v systému z/OS**

Exportujte certifikát pomocí příkazu RACDCERT.

V systému, ze kterého chcete exportovat certifikát, použijte tento příkaz:

```
RACDCERT ID(userid2) EXPORT(LABEL('label-name'))  
DSN(output-data-set-name) FORMAT(CERTB64)
```

kde:

- *userid2* je ID uživatele, pod kterým byl certifikát přidán do svazku klíčů.
- *název-návěští* je jmenovka certifikátu, který chcete extrahovat.
- *název-výstupní-datové-sady* je datová sada, do které je certifikát umístěn.
- CERTB64 je certifikát X.509 kódovaný pomocí DER, který je ve formátu Base64. Můžete zvolit alternativní formát, například:

#### **CERTDER**

certifikát kódovaný pomocí DER X.509 v binárním formátu

#### **PKCS12B64**

Certifikát PKCS #12 ve formátu Base64

#### **PKCS12DER**

Certifikát PKCS #12 v binárním formátu

### **Odstranění osobního certifikátu z úložiště klíčů v systému z/OS**

Odstranění osobního certifikátu pomocí příkazu RACDCERT.

Před odstraněním osobního certifikátu můžete chtít uložit jeho kopii. Chcete-li zkopírovat svůj osobní certifikát do datové sady před jejím odstraněním, postupujte podle pokynů v části “Export osobního certifikátu z úložiště klíčů v systému z/OS” na stránce 310. Pak použijte následující příkaz k odstranění osobního certifikátu:

```
RACDCERT ID( userid2 ) DELETE(LABEL(' label-name '))
```

kde:

- *userid2* je ID uživatele, pod kterým byl certifikát přidán do svazku klíčů.
- *název-návěští* je jméno certifikátu, který chcete vymazat.

### **Přejmenování osobního certifikátu v úložišti klíčů v systému z/OS**

Přejmenujte certifikát pomocí příkazu RACDCERT.

Pokud nechcete, aby byl nalezen certifikát s určitým popiskem, ale nechcete jej odstranit, můžete jej přejmenovat dočasně pomocí následujícího příkazu:

```
RACDCERT ID( userid2 ) LABEL( ' label-name ' ) NEWLABEL( ' new-label-name ' )
```

kde:

- *userid2* je ID uživatele, pod kterým byl certifikát přidán do svazku klíčů.
- Parametr *název-návěští* je název certifikátu, který chcete přejmenovat.
- *new-label-name* je nový název certifikátu.

To může být užitečné při testování ověření klienta SSL.

### **Přidružení ID uživatele k digitálnímu certifikátu v systému z/OS**

IBM MQ může použít ID uživatele přidružené k certifikátu RACF jako ID uživatele kanálu. Přidružte ID uživatele k certifikátu tak, že jej nainstalujete pod toto ID uživatele, nebo pomocí filtru názvu certifikátu.

Metoda popsaná v tomto tématu představuje alternativu k metodě pro přidružení ID uživatele k digitálnímu certifikátu, který používá záznamy ověřování kanálu. Další informace o záznamech ověření kanálu viz [“Záznamy ověření kanálu”](#) na stránce 48.

Když entita na jednom konci kanálu SSL obdrží certifikát od vzdáleného připojení, zobrazí se entita RACF , pokud existuje ID uživatele přidružené k tomuto certifikátu. Entita používá toto ID uživatele jako ID uživatele kanálu. Pokud k certifikátu není přidruženo žádné ID uživatele, bude entita používat ID uživatele, pod kterým je spuštěn inicializátor kanálu.

Přidružte ID uživatele k certifikátu jedním z následujících způsobů:

- Nainstalujte tento certifikát do databáze produktu RACF pod ID uživatele, ke kterému jej chcete přidružit, jak je popsáno v tématu [“Přidání osobních certifikátů do úložiště klíčů v systému z/OS”](#) na stránce 309.
- Použijte CNF (Certificate Name Filter) k mapování rozlišujícího názvu subjektu nebo vydavatele certifikátu na ID uživatele, jak je popsáno v [“Nastavení filtru názvu certifikátu”](#) na stránce 311.

#### *Nastavení filtru názvu certifikátu*

Pomocí příkazu RACDCERT můžete definovat filtr názvů certifikátů (CNF), který mapuje rozlišující název na ID uživatele.

Chcete-li nastavit CNF, proveďte následující kroky.

1. Povolte funkce CNF pomocí následujícího příkazu. K provedení této akce je zapotřebí oprávnění k aktualizaci třídy DIGTNMAP.

```
SETOPTS CLASSACT(DIGTNMAP) RACLIST(DIGTNMAP)
```

2. Definujte CNF. Příklad:

```
RACDCERT ID(USER1) MAP WITHLABEL('filter1') TRUST  
SDNFILTER('O=IBM.C=UK') IDNFILTER('O=ExampleCA.L=Internet')
```

kde USER1 je ID uživatele, které se má použít, když:

- DN subjektu má organizaci IBM a zemi s UK.
- DN vydavatele má organizaci ExampleCA a lokalitou Internet.

3. Aktualizujte mapování CNF:

```
SETOPTS RACLIST(DIGTNMAP) REFRESH
```

#### **Poznámka:**

1. Je-li skutečný certifikát uložen v databázi RACF , použijte se ID uživatele, pod kterým je nainstalován, v preferovaném ID uživatele, který je přidružen k jakémukoli CNF. Není-li certifikát uložen v databázi RACF , použijte se ID uživatele přidružené k nejspecifičtější shodným CNF. Shoduje se s rozlišujícím názvem subjektu, které jsou považovány za specifičtější, než odpovídá rozlišujícímu názvu DN.
2. Změny do CNFs se nepoužijí, dokud neobnovíte mapování CNF.
3. DN se shoduje s filtrem DN v CNF pouze, pokud je filtr DN identický s *nejméně významnou částí* DN. Nejméně významná část DN se skládá z atributů, které jsou obvykle uvedeny na nejspřávnějším konci DN, ale které se objevují na začátku certifikátu.

Vezměme si například příkaz `SDNFILTER 'O=IBM.C=UK'` . Rozlišovací jméno subjektu `'CN=QM1.O=IBM.C=UK'` odpovídá tomuto filtru, ale rozlišující název subjektu `'CN=QM1.O=IBM.L=Hursley.C=UK'` neodpovídá tomuto filtru.

Nejméně významná část některých certifikátů může obsahovat pole, která se neshodují s filtrem DN. Zvažte vyloučení těchto certifikátů uvedením vzoru DN v šabloně `SSLPEEER` v příkazu `DEFINE CHANNEL`.

4. Pokud je nejspecifičtější odpovídající CNF definováno jako `NOTRUST` do RACF , entita používá ID uživatele, pod kterým je spuštěn inicializátor kanálu.
5. RACF používá znak `'.'` jako oddělovač. IBM MQ používá buď čárku, nebo středník.

Můžete definovat CNF, aby se zajistilo, že entita nikdy nenastaví ID uživatele kanálu na výchozí hodnotu, což je ID uživatele, pod kterým je spuštěn inicializátor kanálu. Pro každý certifikát CA v souboru svazku klíčů přidruženém k entitě definujte CNF s parametrem `IDNFILTER`, který přesně odpovídá rozlišujícímu názvu DN daného certifikátu CA. Tím je zajištěno, že všechny certifikáty, které může účetní jednotka použít, se budou shodovat alespoň s jedním z těchto CNFs. Důvodem je to, že všechny tyto certifikáty musí být buď připojeny ke svazku klíčů přidruženému k entitě, nebo musí být vydáno CA, pro který je certifikát připojen k svazku klíčů přidruženému k entitě.

Další informace o příkazech, které používáte k manipulaci s CNFs, naleznete v příručce *SecureWay Security Server RACF Security Administrator's Guide* .

## **Definování kanálu odesílatele a přenosové fronty na QMA**

Chcete-li nastavit vyžadované objekty, použijte příkazy `DEFINE CHANNEL` a `DEFINE QLOCAL` .

### **Postup**

U správce QMA zadejte příkazy jako následující příklad:

```
DEFINE CHANNEL(TO.QMB) CHLTYPE(SDR) TRPTYPE(TCP) CONNAME(QMB.MACH.COM) XMITQ(QMB)
SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA) DESCR('Sender channel using TLS from QMA to QMB')

DEFINE QLOCAL(QMB) USAGE(XMITQ)
```

### **Výsledky**

Kanál odesílatele `TO.QMB`a vytvoří se přenosová fronta `QMB`.

## **Definování přijímacího kanálu na QMB**

Chcete-li nastavit požadovaný objekt, použijte příkaz `DEFINE CHANNEL` .

### **Postup**

V `QMB` zadejte příkaz jako následující příklad:

```
DEFINE CHANNEL(TO.QMB) CHLTYPE(RCVR) TRPTYPE(TCP) SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA)
SSLCAUTH(REQUIRED) DESCR('Receiver channel using TLS to QMB')
```

## Výsledky

Přijímací kanál TO.QMB, je vytvořeno.

### ***Spuštění kanálu odesílatele***

Je-li to nezbytné, spusťte program listener a obnovte zabezpečení. Poté spusťte kanál pomocí příkazu **START CHANNEL**.

## Postup

1. Volitelné: Pokud jste tak dosud neučinili, spusťte program modulu listener na QMB.  
Program modulu listener naslouchá příchozím požadavkům na síť a spouští přijímací kanál, když je potřeba. Informace o tom, jak spustit modul listener, najdete v tématu [Spuštění modulu listener kanálu](#).
2. Volitelné: Pokud již byly spuštěny nějaké kanály zabezpečení SSL nebo TLS, zadejte příkaz **REFRESH SECURITY TYPE(SSL)**.  
Tím je zajištěno, že všechny změny provedené v úložišti klíčů jsou dostupné.
3. Spusťte kanál na QMA pomocí příkazu **START CHANNEL (TO.QMB)**.

## Výsledky

Kanál odesílatele je spuštěn.

### ***Výměna certifikátů s vlastním podpisem***

Vyměňte certifikáty, které jste předtím extrahovali. Používáte-li protokol FTP, použijte správný formát.

## Postup

Přeneste CA část certifikátu QM1 do systému QM2 a opačně, například pomocí FTP.

Pokud přenášejí certifikáty pomocí protokolu FTP, musíte tak učinit ve správném formátu.

Přeneste následující typy certifikátů ve formátu *binary* :

- Binární X.509 kódovaný pomocí DER
- PKCS #7 (certifikáty CA)
- PKCS #12 (osobní certifikáty)

Přeneste následující typy certifikátů ve formátu ASCII:

- PEM (ochrana soukromí-rozšířená pošta)
- Base64 kódováno X.509

### ***Definování kanálu odesílatele a přenosové fronty na systému QM1***

Chcete-li nastavit vyžadované objekty, použijte příkazy **DEFINE CHANNEL** a **DEFINE QLOCAL**.

## Postup

V systému QM1zadejte příkazy jako následující příklad:

```
DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(SDR) TRPTYPE(TCP) CONNAME(QM1.MACH.COM) XMITQ(QM2)
SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA) DESCR('Sender channel using 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.

Pouze parametr SSLCIPH je povinný, pokud chcete, aby kanál používal zabezpečení SSL nebo TLS. Informace o povolených hodnotách pro parametr SSLCIPH naleznete v příručce [“CipherSpecs a CipherSuites v produktu IBM MQ”](#) na stránce 37.

## Výsledky

Odesílací kanál QM1.TO.QM2, a přenosová fronta QM2, se vytvoří.

### **Definování přijímacího kanálu na systému QM2**

Chcete-li nastavit požadovaný objekt, použijte příkaz **DEFINE CHANNEL** .

## Postup

V systému QM2zadejte příkaz podobný tomuto příkladu:

```
DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(RCVR) TRPTYPE(TCP) SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA)
SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL from QM1 to QM2')
```

Kanál musí mít stejný název jako odesílacího kanálu, který jste definovali v produktu “[Definování kanálu odesílatele a přenosové fronty na systému QM1](#)” na stránce 313, a použít stejnou CipherSpec.

### **Spuštění kanálu odesílatele**

Je-li to nezbytné, spusťte program listener a obnovte zabezpečení. Poté spusťte kanál pomocí příkazu **START CHANNEL** .

## Postup

1. Volitelné: Pokud jste tak dosud neučinili, spusťte program modulu listener na systému QM2.  
Program modulu listener naslouchá příchozím požadavkům na síť a spouští přijímací kanál, když je potřeba. Informace o tom, jak spustit modul listener, najdete v tématu [Spuštění modulu listener kanálu](#) .
2. Volitelné: Pokud byly dříve spuštěny žádné kanály SSL nebo TLS, zadejte příkaz **REFRESH SECURITY TYPE (SSL)**.  
Tím je zajištěno, že všechny změny provedené v úložišti klíčů jsou dostupné.
3. V systému QM1spusťte kanál pomocí příkazu **START CHANNEL (QM1 . TO . QM2)**.

## Výsledky

Kanál odesílatele je spuštěn.

### **Aktualizace prostředí SSL nebo TLS**

Aktualizujte prostředí SSL nebo TLS ve správci front QMA pomocí příkazu **REFRESH SECURITY** .

## Postup

Na správci QMA zadejte tento příkaz:

```
REFRESH SECURITY TYPE(SSL)
```

Tím je zajištěno, že všechny změny provedené v úložišti klíčů jsou dostupné.

### **Povolení anonymních připojení k přijímacímu kanálu**

Použijte příkaz **ALTER CHANNEL** , abyste učinili ověření klienta SSL nebo TLS volitelné.

## Postup

Na QMB zadejte tento příkaz:

```
ALTER CHANNEL(TO.QMB) CHLTYPE(RCVR) SSLCAUTH(OPTIONAL)
```

## ***Spuštění kanálu odesílatele***

V případě potřeby spusťte iniciátor kanálu, spusťte program modulu listener a obnovte zabezpečení. Poté spusťte kanál pomocí příkazu **START CHANNEL** .

### **Postup**

1. Volitelné: Pokud jste tak dosud neučinili, spusťte iniciátor kanálu.
2. Volitelné: Pokud jste tak dosud neučinili, spusťte program modulu listener na systému QM2.  
Program modulu listener naslouchá příchozím požadavkům na síť a spouští přijímací kanál, když je potřeba. Informace o tom, jak spustit modul listener, najdete v tématu [Spuštění modulu listener kanálu](#) .
3. Volitelné: Pokud byl inicializátor kanálu již spuštěn nebo byly již dříve spuštěny žádné kanály zabezpečení SSL nebo TLS, zadejte příkaz REFRESH SECURITY TYPE (SSL).  
Tím je zajištěno, že všechny změny provedené v úložišti klíčů jsou dostupné.
4. V systému QM1 spusťte kanál pomocí příkazu START CHANNEL (QM1 . TO . QM2) .

### **Výsledky**

Kanál odesílatele je spuštěn.

## ***Spuštění kanálu odesílatele v systému z/OS***

V případě potřeby spusťte iniciátor kanálu, spusťte program modulu listener a obnovte zabezpečení. Poté spusťte kanál pomocí příkazu **START CHANNEL** .

### **Postup**

1. Volitelné: Pokud jste tak dosud neučinili, spusťte iniciátor kanálu.
2. Volitelné: Pokud jste tak dosud neučinili, spusťte program modulu listener na QMB.  
Program modulu listener naslouchá příchozím požadavkům na síť a spouští přijímací kanál, když je potřeba. Informace o tom, jak spustit modul listener, najdete v tématu [Spuštění modulu listener kanálu](#) .
3. Volitelné: Pokud byl inicializátor kanálu již spuštěn nebo pokud již některé kanály zabezpečení SSL nebo TLS byly spuštěny dříve, zadejte příkaz REFRESH SECURITY TYPE (SSL) .  
Tím je zajištěno, že všechny změny provedené v úložišti klíčů jsou dostupné.
4. Spusťte kanál na QMA pomocí příkazu START CHANNEL (TO . QMB) .

### **Výsledky**

Kanál odesílatele je spuštěn.

## **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 MQCONN; tato struktura obsahuje ID uživatele a heslo. Je-li to nutné, můžete změnit MQCSP v uživatelské proceduře zabezpečení.

**Poznámka:** Správce oprávnění k objektu (OAM) nepoužívá heslo. Avšak OAM má určitou omezenou práci s ID uživatele, které lze považovat za triviální formu ověření. Tyto kontroly přestanou přijímat další ID uživatele, používáte-li tyto parametry ve svých aplikacích.

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



## Implementace identifikace a ověření v uživatelských procedurách zabezpečení

Primárním účelem uživatelské procedury zabezpečení je umožnit agentovi MCA na každém konci kanálu ověřovat jeho partnera. Na každém konci kanálu zpráv a na konci kanálu kanálu MQI agent MCA obvykle jedná jménem správce front, ke kterému je připojen. Na konci klienta kanálu MQI se agent MCA obvykle chová jménem uživatele klientské aplikace produktu IBM MQ. V této situaci probíhá vzájemná ověření mezi dvěma správci front nebo mezi správcem front a uživatelem aplikace produktu IBM MQ MQI client.

Dodaná uživatelská procedura zabezpečení (uživatelská procedura kanálu SSPI) ilustruje, jak lze vzájemné ověření implementovat pomocí výměny tokenů ověření, které jsou generovány, a poté zkontrolovány důvěryhodným ověřovacím serverem, jako je například Kerberos. Další informace naleznete v tématu [“Ukončovací program kanálu SSPI”](#) na stránce 139.

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 provádět ověření, viz [“Koncepte 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 401. 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 102.

Všechny předchozí techniky pro vzájemné ověření mohou být přizpůsobeny tak, aby poskytovaly jednosměrné ověření.

## Implementace identifikace a ověření ve výstupních procedurách zprávy

Když aplikace vloží zprávu do fronty, pole *UserIdentifier* v deskriptoru zprávy obsahuje ID uživatele přidružené k aplikaci. Avšak nejsou přítomna žádná data, která by mohla být použita k ověření ID uživatele. Tato data mohou být přidána uživatelskou procedurou pro odeslání zprávy na odesílající straně kanálu a kontrolována ukončením zprávy na přijímajícím konci kanálu. Ověřující data mohou být šifrovaným heslem nebo digitálním podpisem, například.

Tato služba může být efektivnější, pokud je implementována na úrovni aplikace. Základním požadavkem je pro uživatele aplikace, která přijímá zprávu, aby bylo možné identifikovat a ověřit uživatele aplikace, která odeslala zprávu. Je proto přirozené zvážit zavedení této služby na úrovni aplikace. Další informace viz [“Mapování identity ve výstupu rozhraní API a ukončení přeletu rozhraní API”](#) na stránce 321.

## 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 odesílatel, 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 odesílatele 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 odesílatele. Další možností je odeslat všechny certifikáty v řetězu certifikátů.

- Když aplikace vloží zprávu do fronty, pole *UserIdentifier* v deskriptoru zprávy obsahuje ID uživatele přidružené k aplikaci. ID uživatele lze použít k identifikaci odesílatele. Chcete-li povolit ověření, může uživatelská procedura rozhraní API připojit některá data, jako je například zašifrované heslo, k datům aplikace ve zprávě. Když je zpráva načtena přijímající aplikací, druhá uživatelská procedura rozhraní API může ověřit ID uživatele pomocí dat, která se urazila se zprávou.

Tato technika může být považována za dostatečnou pro zprávy, které pocházejí z řízeného a důvěryhodného prostředí, a za okolností, kdy není k dispozici důvěryhodný ověřovací server nebo podpora PKI.

## PAM (Pluggable Authentication Method)



Modul PAM je nyní běžný na všech platformách SYSTÉM UNIX a Linux a poskytuje obecný mechanismus, který skrývá podrobnosti o ověření uživatele ze služeb.

Pro různé služby lze použít různá pravidla ověření, a to konfigurací pravidel, bez nutnosti změn pro samotné služby.


Další informace viz [“Použití metody PAM \(Pluggable Authentication Method\)”](#) na stránce 333.

## Oprávnění uživatelé

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

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

Tato oprávnění byste neměli udělovat běžným uživatelům a aplikacím.

<i>Tabulka 66. Oprávnění uživatelé podle platformy</i>	
Platforma	Oprávnění uživatelé
Systémy Windows	<ul style="list-style-type: none"> <li>• SYSTÉM</li> <li>• Členové skupiny mqm</li> <li>• Členové skupiny administrátorů</li> </ul>
Systémy SYSTÉM UNIX a Linux	<ul style="list-style-type: none"> <li>• Členové skupiny mqm</li> </ul>
 Systémy IBM i	<ul style="list-style-type: none"> <li>• Profily qmqm a qmqmadm</li> <li>• Všechny členy skupiny qmqmadm</li> <li>• Jakýkoli uživatel definovaný s nastavením *ALLOBJ</li> </ul>
z/OS	ID uživatele, pod kterým jsou spuštěny adresní prostory pro iniciátor kanálu, správce front a rozšířené zabezpečení zpráv.

## Identifikace a ověřování uživatelů pomocí struktury MQCSP

Strukturu parametrů zabezpečení připojení MQCSP můžete zadat na volání MQCONN.

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

V uživatelské proceduře zabezpečení můžete změnit MQCSP.

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

### Relace mezi MQCSP a nastaveními AdoptCTX

Produkt IBM MQ vždy ověřuje pověření předávaná prostřednictvím struktury MQCSP, není-li funkce ověření připojení povolena. Jakmile jsou pověření úspěšně ověřena, produkt IBM MQ se pokusí přijmout ID uživatele pro budoucí kontroly autorizace, pokud není povolena volba ADOPTCTX.

IBM MQ má omezení délky ID uživatelů, které může uživatel použít pro kontrolu autorizace. Tyto limity jsou podrobně popsány na [“ID uživatelů”](#) na stránce 70. Při převzetí ID uživatele předávaného strukturou MQCSP IBM MQ se chová jinak, v závislosti na jiných volbách konfigurace:

- Při použití ověření připojení pomocí protokolu LDAP produkt IBM MQ načte hodnotu pole nastaveného v parametru SHORTUSR ze záznamu LDAP uživatele tohoto uživatele a převezme toto ID uživatele.

Je-li například parametr SHORTUSR nastaven na hodnotu 'CN' a záznam LDAP vypisuje uživatele jako 'CN=Test,SN=MQ,O=IBM,C=UK', použije se ID uživatele Test.

- Pokud používáte ověření připojení operačního systému nebo ověření PAM, je-li parametr ADOPTCTX nastaven na hodnotu YES, bude ID uživatele předané prostřednictvím struktury MQCSP zkráceno, aby bylo při adopci jako kontext připojení dosaženo 12 znaků omezení ID uživatele produktu IBM MQ.

Je-li volba **Ch1AuthEarlyAdopt** povolena, bude zkrácení provedeno poté, co byla ověřena uživatelská pověření.

Není-li volba **Ch1AuthEarlyAdopt** povolena, dojde k oříznutí před přijetím. On Windows, if the user is supplied in the format `user@domain`, this means that the truncation can result in a domain specification that is not valid when the user is less than 12 characters.

Je-li například uživatel ``ibmmq@windowsdomain`` poskytován prostřednictvím MQCSP, je v tomto scénáři zkrácen na ``ibmmq@window``. Výsledkem je následující chyba:

```
AMQ8074W: Autorizace se nezdařila, protože SID 'SID' neodpovídá entitě 'ibmmq@window'
```

Na tomto základě, pokud předáváte ID uživatele delší než 12 znaků, například ID uživatele domény produktu Windows ve tvaru `user@domain`, prostřednictvím MQCSP byste měli nakonfigurovat **Ch1AuthEarlyAdopt=Y** v souboru `qm.ini`, abyste se této chybě vyhnuli.

Případně můžete na konfiguraci CONNAUTH AUTHINFO použít příkaz ADOPTCTX (NO) a použít alternativní přístup, jako je například pravidlo CHLAUTH USERMAP, ukončení zabezpečení nebo nastavení MCAUSER objektu kanálu, a nastavit tak ID uživatele pro kanál.

## Implementace identifikace a ověření v uživatelských procedurách zabezpečení

Ukončení zabezpečení můžete použít k implementaci jednosměrného nebo vzájemného ověření.

Primárním účelem uživatelské procedury zabezpečení je umožnit agentovi MCA na každém konci kanálu ověřovat jeho partnera. Na každém konci kanálu zpráv a na konci kanálu MQI agent MCA obvykle jedná jménem správce front, ke kterému je připojen. Na konci klienta kanálu MQI se agent MCA obvykle chová jménem uživatele aplikace IBM MQ MQI client. V této situaci probíhá vzájemná ověření mezi dvěma správci front nebo mezi správcem front a uživatelem aplikace produktu IBM MQ MQI client.

Dodaná uživatelská procedura zabezpečení (uživatelská procedura kanálu SSPI) ilustruje, jak lze vzájemné ověření implementovat pomocí výměny tokenů ověření, které jsou generovány, a poté

zkontrolovány důvěryhodným ověřovacím serverem, jako je například Kerberos. Další informace naleznete v tématu [“Ukončovací program kanálu SSPI”](#) na stránce 139.

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 zabezpečení SSL provádí ověřování, najdete v tématu [“Koncepte 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 401. 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 102.

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 321.

## 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 odesílatel, 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 odesílatele 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 odesílatele. Další možností je odeslat všechny certifikáty v řetězu certifikátů.



- Když aplikace vloží zprávu do fronty, pole *UserIdentifier* v deskriptoru zprávy obsahuje ID uživatele přidružené k aplikaci. ID uživatele lze použít k identifikaci odesílatele. Chcete-li povolit ověření, 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 vydavatelem 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) odvolávají 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).

Na následujících platformách IBM MQ zabezpečení SSL 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.

-  Linux
-  UNIX
-  Windows

Produkty IBM MQ classes for Java a IBM MQ classes for JMS nemohou používat informace OCSP v souboru s tabulkou definic kanálů klienta. Nicméně můžete OCSP nakonfigurovat podle popisu uvedeného v tématu [Používání protokolu certifikátů online](#).

Na následujících platformách a podpora zabezpečení SSL produktu IBM MQ kontroluje odvolané certifikáty pomocí seznamů CRL a ARL pouze na serverech LDAP:

-  IBM i
-  z/OS

Další informace o certifikačních autorech najdete v tématu [“digitální certifikáty” na stránce 9](#).

## Kontrola OCSP/CRL

Kontrola protokolu OCSP (Online Certificate Status Protocol) /CRL (Certificate Revocation List) se provádí proti vzdáleným příchozím certifikátům. Proces zkontroluje celý řetězec, který se podílí na osobním certifikátu vzdáleného systému, až po jeho kořenový certifikát.

## Jak pracuje kontrola OCSP/CRL v produktu IBM MQ?

Produkt IBM MQ podporuje dva mechanismy pro řízení chování při kontrole certifikátů proti pojmenovaným koncovým bodům OCSP nebo CRL, a to buď v rozšíření certifikátu, nebo v případě, že jsou definovány v objektech AUTHINFO:

- Atributy **OCSPCheckExtensions**, **CDPCheckExtensions** a **OCSPAuthentication** ze sekce [SSL](#) souboru [qm.inia](#)

- Použití parametru `SSLCRLNL` správce front a konfigurací OCSP a CRLLDAP protokolu AUTHINFO. Další informace viz [ALTER AUTHINFO](#) a [ALTER QMGR](#).



### Upozornění:

Příkaz `ALTER AUTHINFO` s produktem **AUTHTYPE (OCSP)** se nepoužívá pro použití ve správcích front IBM i nebo z/OS. Lze však zadat na těchto platformách, aby se zkopírovaly do tabulky definic kanálů klienta (CCDT) pro klientské použití.

Atributy stano **OCSPCheckExtensions** a **CDPCheckExtensions** SSL řídí, zda produkt IBM MQ ověří certifikát proti protokolu OCSP nebo serveru CRL, který je podrobně popsán v rozšíření certifikátu AIA certifikátu.

Není-li tato možnost povolena, protokol OCSP nebo CRL v rozšíření certifikátu se nekontaktuje.

Pokud jsou protokoly OCSP nebo CRL podrobně popsány pomocí objektů AUTHINFO a odkazovány pomocí atributu `SSLCRLNL QMGR`, pak během zpracování odvolání certifikátů se produkt IBM MQ pokusí kontaktovat tyto servery.

**Důležité:** V seznamu názvů `SSLCRLNL` může být definován pouze jeden objekt OCSP AUTHINFO.

Pokud:

**OCSPCheckExtensions=NO** a **CDPCheckExtensions=NO** jsou nastaveny a  
V objektech AUTHINFO nejsou definovány žádné servery OCSP nebo CRL

neprovádí se žádná kontrola odvolání certifikátu.

Při ověřování certifikátu pro jeho stav odvolání produkt IBM MQ kontaktuje protokol OCSP nebo seznam serverů CRL uvedený v následujícím pořadí, pokud je povolen:

1. Server OCSP je podrobně popsán v objektu **AUTHTYPE (OCSP)** a odkazuje se v atributu `SSLCRLNL QMGR`.
2. Servery OCSP podrobně uvedené v rozšíření AIA certifikátů, pokud je **OCSPCheckExtensions=YES**.
3. Servery CRL jsou podrobně popsány v rozšíření **CRLDistributionPoints** certifikátů, pokud je **CDPCheckExtensions=YES**.
4. Všechny servery CRL, které jsou podrobně popsány v objektech **AUTHINFO (CRLLDAP)** a jsou odkazovány v atributu `SSLCRLNL QMGR`.

Při ověřování certifikátu se v případě, že krok na serveru OCSP nebo na serveru CRL vrátí definitivní odpověď `REVOKED` nebo `VALID` na dotaz na certifikát, neprovedou se žádné další kontroly a stav certifikátu, jak je prezentován, se používá k určení, zda mu důvěřovat, či nikoli.

Pokud server OCSP nebo server CRL vrátí výsledek `UNKNOWN`, zpracování pokračuje, dokud server OCSP nebo CRL nevrátí konečný výsledek, nebo jsou vyčerpány všechny možnosti.

Chování, zda je certifikát považován za zrušený, nelze-li jeho stav určit, se liší pro OCSP a servery CRL:

- Pro servery CRL, pokud nelze získat seznam CRL, je certifikát považován za `NOT_REVOKED`
- Pokud v případě serverů OCSP nelze získat stav odvolání z pojmenovaného serveru OCSP, bude chování řízeno atributem **OCSPAuthentication** v sekci SSL Stanza souboru `qm.ini`.

Tento atribut můžete nakonfigurovat tak, aby blokoval připojení, povolit připojení nebo povolit připojení s varovnou zprávou.

Podle potřeby můžete použít atribut **SSLHTTPProxyName=string** ve stanze SSL souboru `qm.ini` a `mqclient.ini` pro kontroly OCSP. Řetězec je buď název hostitele, nebo síťová adresa serveru proxy HTTP, který má sada GSKit použít pro kontroly OCSP.

## Zrušené certifikáty and OCSP

Produkt IBM MQ zjišťuje, který odpovídací modul protokolu OCSP (Online Certificate Status Protocol) má použít, a zpracovává přijatou odezvu. V některých případech je nutné provést kroky, kterými zpřístupníte odpovídací modul OCSP.



**Poznámka:** Tyto informace platí pouze pro IBM MQ v systémech Windows, SYSTÉM UNIX a Linux .

Chcete-li zkontrolovat stav odvolání digitálního certifikátu pomocí protokolu OCSP, produkt IBM MQ může použít dvě metody k určení odpovídajícího 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 odpovídajícího modulu OCSP za branou firewall, změňte konfiguraci brány firewall tak, aby k odpovídajícímu modulu OCSP bylo možné přistupovat, nebo zřídte 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 odpovídajícímu modulu OCSP může vyvolat jeden z těchto tří výsledků:

#### **Platný**

Certifikát je platný.

#### **Zrušený**

Certifikát je zrušený.

#### **Neznámý**

Tento výsledek se může vyskytnout ze tří různých příčin:

- Produkt IBM MQ nezískal přístup k odpovídajícímu modulu OCSP.
- Odpovídající modul OCSP odeslal odezvu, ale produktu IBM MQ se nepodařilo ověřit digitální podpis této odezvy.
- Odpovídající modul OCSP odeslal odezvu s informací, že nemá k dispozici žádná data o odvolání daného certifikátu.

Obdrží-li produkt IBM MQ výsledek protokolu OCSP Neznámý, jeho chování bude záviset na nastavení atributu OCSPAuthentication. Pro správce front je tento atribut zadržen ve stanze SSL souboru qm. ini pro systémy SYSTÉM UNIX a Linux nebo v registru Windows . Lze ji nastavit pomocí Průzkumníka IBM 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 IBM MQ připojení odmítne a vydá chybovou zprávu typu AMQ9716. Jsou-li povoleny zprávy o událostech správce front SSL, dojde k vygenerování zprávy o události SSL typu MQRC\_CHANNEL\_SSL\_ERROR s atributem ReasonQualifier nastaveným na hodnotu MQRC\_SSL\_HANDSHAKE\_ERROR.

Je-li přijat výsledek Neznámý a atribut OCSPAuthentication je nastaven na hodnotu OPTIONAL, produkt IBM MQ umožní spuštění kanálu SSL a nebudou vygenerována žádná varování ani zprávy o událostech SSL.

Je-li přijat výsledek Neznámý a atribut OCSPAuthentication je nastaven na hodnotu WARN, kanál SSL se spustí, ale produkt IBM MQ zapíše do protokolu chyb varovnou zprávu typu AMQ9717. Jsou-li povoleny zprávy o událostech správce front SSL, dojde k vygenerování zprávy o události SSL typu MQRC\_CHANNEL\_SSL\_WARNING s atributem ReasonQualifier nastaveným na hodnotu MQRC\_SSL\_UNKNOWN\_REVOCATION.

## Digitální podepisování odezev OCSP

Odpověď modul OCSP může své odezvy podepisovat jedním ze tří způsobů. Váš odpověď 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 odpověďovacího 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 odpověďovacím modulem OCSP. Kopii certifikátu odpověďovacího modulu OCSP je nutné přidat do databáze klíčů klienta nebo správce front, který provádí kontrolu OCSP. Přidávaný certifikát CA je standardně přidán jako důvěryhodný kořenový certifikát, což je v tomto kontextu povinné nastavení. Není-li tento certifikát přidán, produkt IBM MQ nemůže ověřit digitální podpis v odezvě OCSP a kontrola protokolu OCSP má za následek Neznámý výsledek, který může způsobit zavření kanálu produktem IBM MQ v závislosti na hodnotě prvku `OCSPAuthentication`.

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

Kvůli omezení rozhraní API produktu Java může produkt IBM MQ použít kontrolu odvolání certifikátů protokolu OCSP (Online Certificate Status Protocol) pro zabezpečené sokety SSL a TLS pouze v případě, že je protokol OCSP povolen pro celý proces virtuálního počítače 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 soubor `java.security.Security.setProperty()` Rozhraní API, v závislosti na platné zásadě produktu Java Security Manager.

Přínejmenším musíte zadat jednu z hodnot `ocsp.enable` a `ocsp.responderURL`.

Název vlastnosti	Popis
<code>ocsp.enable</code>	Tato vlastnost má hodnotu <code>true</code> nebo <code>false</code> . Je-li použita hodnota <code>true</code> , je kontrola OCSP povolena při kontrole odvolání certifikátu. Je-li použita hodnota <code>false</code> nebo není-li vlastnost nastavena vůbec, je kontrola OCSP vypnuta.
<code>ocsp.responderURL</code>	Tato vlastnost nese hodnotu, jež odpovídá adrese URL, která určuje umístění odpověďovacího modulu OCSP. Příklad: <code>ocsp.responderURL=http://ocsp.example.net:80</code> . Při výchozím nastavení se umístění odpověďovacího 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.
<code>ocsp.responderCertSubjectName</code>	Tato vlastnost nese hodnotu, jež určuje název subjektu certifikátu odpověďovacího modulu OCSP. Příklad: <code>ocsp.responderCertSubjectName="CN=OCSP Responder, O=XYZ Corp"</code> . Při výchozím nastavení certifikát odpověďovacího modulu OCSP má vydavatele, který vydal ověřovaný certifikát. Tato vlastnost identifikuje certifikát odpověďovacího modulu OCSP v případě, že nelze použít výchozí hodnotu. Jeho hodnota je

Název vlastnosti	Popis
	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: <code>ocsp.responderCertIssuerName</code> a <code>ocsp.responderCertSerialNumber</code> . Je-li tato vlastnost nastavena, budou vlastnosti <code>ocsp.responderCertIssuerName</code> a <code>ocsp.responderCertSerialNumber</code> ignorovány.
<code>ocsp.responderCertIssuerName</code>	Tato vlastnost nese hodnotu odpovídající názvu vydavatele certifikátu odpovídajícího modulu OCSP. Příklad: <code>ocsp.responderCertIssuerName="CN=Enterprise CA, O=XYZ Corp"</code> . Při výchozím nastavení certifikát odpovídajícího modulu OCSP má vydavatele, který vydal ověřovaný certifikát. Tato vlastnost identifikuje certifikát odpovídajícího 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 <code>ocsp.responderCertSerialNumber</code> . Tato vlastnost je ignorována, je-li nastavena vlastnost <code>ocsp.responderCertSubjectName</code> .
<code>ocsp.responderCertSerialNumber</code>	Tato vlastnost nese hodnotu, jež je sériovým číslem certifikátu odpovídajícího modulu OCSP. Příklad: <code>ocsp.responderCertSerialNumber=2A:FF:00</code> . Při výchozím nastavení certifikát odpovídajícího modulu OCSP má vydavatele, který vydal ověřovaný certifikát. Tato vlastnost identifikuje certifikát odpovídajícího 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 <code>ocsp.responderCertIssuerName</code> . Tato vlastnost je ignorována, je-li nastavena vlastnost <code>ocsp.responderCertSubjectName</code> .

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`. Dávejte pozor, když použijete prozatímní opravy produktu Java a údržbu produktu, abyste se vyhnuli přepsání souboru `java.security`. Po použití balíčku údržby může být nezbytné znovu provést vlastní změny v souboru `java.security`. Z tohoto důvodu může být výhodnější provést nastavení konfigurace OCSP prostřednictvím rozhraní API `java.security.Security.setProperty()`.
- Povolení kontroly OCSP se projeví pouze v případě, že je povolena rovněž kontrola odvolání. Kontrola odvolání se povoluje metodou `PKIXParameters.setRevocationEnabled()`.
- Používáte-li komponentu AMS Java Interceptor popsanou v tématu [Povolení kontroly OCSP v nativních zachytávačích](#), dbejte na to, abyste se vyhnuli použití konfigurace protokolu OCSP `java.security`, která je v konfliktu s konfigurací AMS OCSP v konfiguračním souboru úložiště klíčů.

## Práce se seznamy odvolaných certifikátů a seznamy odvolaných autorit

Podpora IBM MQ pro seznamy CRL a ARL se liší podle platformy.

Podpora CRL a ARL na každé platformě je následující:

- V systému z/OSSystem SSL podporuje seznamy CRL a ARL uložené na serverech LDAP produktem Tivoli Public Key Infrastructure.
- Na jiných platformách podpora CRL a ARL odpovídá doporučením profilu PKIX X.509 V2 profilu CRL.

Produkt IBM MQ udržuje mezipaměť seznamů CRL a ARL, k nimž bylo přistupována během předchozích 12 hodin.

Když správce front nebo IBM MQ MQI client obdrží certifikát, zkontroluje seznam CRL a potvrdí, že je certifikát stále platný. IBM MQ první kontroly v mezipaměti, pokud existuje mezipaměť. Pokud seznam CRL není uložen v mezipaměti, produkt IBM MQ dotazuje umístění serveru LDAP CRL v pořadí, v jakém se vyskytují v seznamu názvů objektů ověřovacích informací určených atributem `SSLCRLNL`, dokud produkt IBM MQ nenajde dostupný seznam CRL. Není-li seznam názvů zadán nebo je-li zadán s prázdnou hodnotou, seznamy odvolaných certifikátů se nekontrolují.

## Nastavení serverů LDAP

Konfigurujte strukturu stromu informací adresáře LDAP tak, aby odrážela hierarchii rozlišujících názvů certifikačních autorit. To lze provést pomocí souborů formátu výměny dat LDAP.

Konfigurujte strukturu DIT (Directory Information Tree) LDAP pro použití hierarchie odpovídající rozlišujícím názvům certifikačních úřadů, které vydávají certifikáty a seznamy CRL. Strukturu DIT můžete nastavit pomocí souboru, který používá formát LDIF (LDAP Data Interchange Format). K aktualizaci adresáře můžete také použít soubory LDIF.

Soubory LDIF jsou textové soubory ASCII, které obsahují informace požadované pro definování objektů v rámci adresáře LDAP. Soubory LDIF obsahují jednu nebo více záznamů, z nichž každá obsahuje rozlišující název, alespoň jednu definici třídy objektu a volitelně více definic atributu.

Atribut `certificateRevocationList;binary` obsahuje v binární formě seznam odvolaných uživatelských certifikátů. Atribut `authorityRevocationList;binary` obsahuje binární seznam certifikátů CA, které byly odvolány. Pro použití s SSL IBM MQ musí binární data pro tyto atributy odpovídat formátu DER (Definite Encoding Rules). Další informace o souborech LDIF najdete v dokumentaci dodávané se serverem LDAP.

Obrázek 20 na stránce 327 ukazuje vzorový soubor LDIF, který můžete vytvořit jako vstup na server LDAP pro načtení seznamů CRL a ARL vydaných CA1, což je fiktivní vydavatel certifikátů s rozlišujícím názvem "CN=CA1, OU=Test, O=IBM, C=GB", který je nastaven organizací Test v rámci produktu IBM.

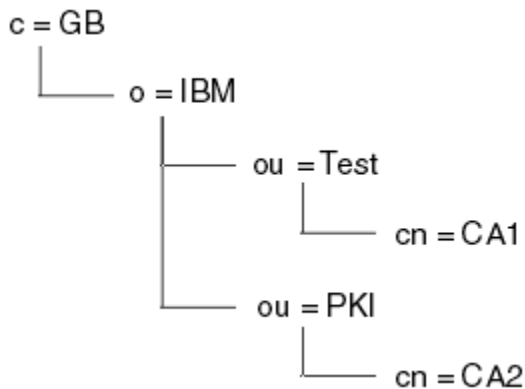
```
dn: o=IBM, c=GB
o: IBM
objectclass: top
objectclass: organization

dn: ou=Test, o=IBM, c=GB
ou: Test
objectclass: organizationalUnit

dn: cn=CA1, ou=Test, o=IBM, c=GB
cn: CA1
objectclass: cRLDistributionPoint
objectclass: certificateAuthority
authorityRevocationList;binary:: (DER format data)
certificateRevocationList;binary:: (DER format data)
caCertificate;binary:: (DER format data)
```

*Obrázek 20. Ukázkový soubor LDIF pro certifikační autoritu. To se může lišit od implementace k implementaci.*

Obrázek 21 na stránce 328 ukazuje strukturu DIT, kterou váš server LDAP vytváří při načtení ukázkového souboru LDIF zobrazeného v produktu Obrázek 20 na stránce 327 společně s podobným souborem pro CA2, imaginárním certifikačním úřadem, který je nastaven organizací PKI, také v rámci IBM.



Obrázek 21. Příklad struktury informačního stromu adresáře LDAP

Produkt 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 328.

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 značkám CRL a ARL se správcem front

Správce front je přidružen k jednomu nebo více objektům ověřovacích informací, které uchovávají adresu serveru LDAP CRL.  Produkt Websphere MQ na systému IBM i se chová jinak než ostatní platformy.

Všimněte si, že v této sekci se informace o seznamech CRL (Certificate Revocation Lists) vztahují také na seznamy odvolaných autorit (ARLs).

Správci front sděáte, jak přistupovat k seznamu CRL, zadáním správce front s objekty ověřovacích informací, z nichž každý uchovává adresu serveru LDAP CRL. Objekty ověřovacích informací se nacházejí v seznamu názvů, který je zadán v atributu správce front `SSLCRLNL`.

V následujícím příkladu se používá MQSC pro uvedení parametrů:

1. Definujte objekty ověřovacích informací pomocí příkazu `DEFINE AUTHINFO MQSC` s parametrem `AUTHTYPE` nastaveným na `CRLLDAP`.  V systému IBM i můžete také použít příkaz `CL CRTMQMAUTI`.

Hodnota `CRLLDAP` pro parametr `AUTHTYPE` indikuje, že k seznamům CRL se přistupuje na serverech LDAP. Každý objekt ověřovacích informací s typem `CRLLDAP`, který vytvoříte, obsahuje adresu serveru

LDAP. Máte-li více než jeden objekt ověřovacích informací, servery LDAP, na které odkazují *musí* obsahovat stejné informace. Tato funkce zajišťuje kontinuitu služby, pokud selže jeden nebo více serverů LDAP.

**z/OS** Navíc, pouze v systému z/OS musí být přístup ke všem serverům LDAP používán se stejným ID uživatele a heslem. Použité ID uživatele a heslo jsou uvedeny v prvním objektu AUTHINFO v seznamu názvů.

Na všech platformách se ID uživatele a heslo posílají na server LDAP nešifrovaně.

2. Pomocí příkazu DEFINE NAMELIST MQSC definujte seznam názvů pro názvy objektů ověřovacích informací. **z/OS** V systému z/OS se ujistěte, že atribut seznamu názvů NLTYPE je nastaven na hodnotu AUTHINFO.
3. Pomocí příkazu ALTER QMGR MQSC zadejte seznam názvů do správce front. Příklad:

```
ALTER QMGR SSLCRLNL(sslcrlnlname)
```

kde `sslcrlnlname` je váš seznam názvů objektů ověřovacích informací.

Tento příkaz nastavuje atribut správce front s názvem `SSLCRLNL`. Počáteční hodnota správce front pro tento atribut je prázdná.

**IBM i** V systému IBM můžete zadat objekty ověřovacích informací, ale správce front nepoužívá objekty ověřovacích informací ani seznam názvů objektů ověřovacích informací. Pouze IBM MQ klienti používající tabulku připojení klienta vygenerovanou správcem front produktu IBM i používají informace o ověření určené pro daného správce front IBM i. Atribut správce front `SSLCRLNL` na systému IBM i určuje, jaké informace o ověření používají klienti. See [“Přístup k seznačkám CRL a ARL v systému IBM i”](#) na stránce 329 for information about telling an IBM i queue manager how to access CRLs.

Do seznamu názvů můžete přidat až 10 připojení k alternativním serverům LDAP, abyste zajistili nepřetržitost služby, pokud selže jeden nebo více serverů LDAP. Všimněte si, že servery LDAP *musí* obsahovat identické informace.

#### *Přístup k seznačkám CRL a ARL v systému IBM i*

Tuto proceduru použijte pro přístup k CRL nebo ARL na IBM i.

Všimněte si, že v této sekci se informace o seznamech CRL (Certificate Revocation Lists) vztahují také na seznamy odvolaných autorit (ARLs).

Chcete-li nastavit umístění CRL pro určitý certifikát v systému IBM i, postupujte takto:

1. Přistupte k rozhraní DCM, jak je popsáno v tématu [“Přístup k DCM”](#) na stránce 262.
2. V kategorii úloh **Správa umístění CRL** v navigačním panelu klepněte na volbu **Přidat umístění CRL**. Stránka Správa umístění CRL se zobrazí v rámci úlohy.
3. Do pole **Název umístění CRL** zadejte název umístění CRL, například LDAP Server #1.
4. Do pole **Server LDAP** zadejte název serveru LDAP.
5. V poli **Použití zabezpečení SSL (Secure Sockets Layer)** vyberte volbu **Ano**, chcete-li se připojit k serveru LDAP pomocí SSL. V opačném případě vyberte volbu **Ne**.
6. Do pole **Číslo portu** zadejte číslo portu pro server LDAP, například 389.
7. Pokud váš server LDAP neumožňuje anonymním uživatelům zadávat dotazy na adresář, zadejte přihlašovací rozlišující název serveru do pole **Přihlašovací rozlišující název**.
8. Klepněte na tlačítko **OK**. Produkt DCM vás informuje o tom, že vytvořil umístění CRL.
9. V navigačním panelu klepněte na **Výběr úložiště certifikátů**. V rámci úlohy se zobrazí stránka Výběr úložiště certifikátů.
10. Označte zaškrťovací políčko **Další systémové úložiště certifikátů** a klepněte na **Pokračovat**. Zobrazí se stránka Paměť certifikátů a heslo.

11. V poli **Cesta k úložišti certifikátů a název souboru** zadejte cestu k souboru IFS a název souboru, který jste nastavili při [“Vytvoření úložiště certifikátů v systému IBM i”](#) na stránce 264.
12. Do pole **Heslo úložiště certifikátů** zadejte heslo. Klepněte na tlačítko **Pokračovat**. V rámci úlohy se zobrazí stránka Aktuální úložiště certifikátů.
13. V kategorii úloh **Správa certifikátů** v navigačním panelu klepněte na volbu **Aktualizovat přiřazení umístění CRL**. Stránka Přiřazení umístění CRL se zobrazí v rámci úlohy.
14. Vyberte přepínač pro certifikát CA, ke kterému chcete přiřadit umístění CRL. Klepněte na **Aktualizace přiřazení umístění CRL**. Stránka Aktualizace přiřazení umístění CRL se zobrazí v rámci úlohy.
15. Vyberte přepínač pro umístění CRL, které chcete přiřadit k certifikátu. Klepněte na tlačítko **Aktualizovat přiřazení**. Produkt DCM vás informuje o tom, že aktualizoval přiřazení.

Všimněte si, že produkt DCM vám umožňuje přiřadit jiný server LDAP certifikačním úřadem.

#### *Přístup k seznamům CRL a ARL pomocí Průzkumníka IBM MQ*

Průzkumník IBM MQ můžete použít k tomu, abyste správci front sdělili, jak přistupovat k seznamovým seznamu úloh 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 **Namelist** 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 330) do seznamu.
  - c. Klepněte na tlačítko **OK**.
4. Klepněte pravým tlačítkem myši na správce front, vyberte volbu **Vlastnosti** poté vyberte stránku **SSL** :
  - a. Vyberte zaškrťovací políčko **Zkontrolovat certifikáty přijaté tímto správcem front proti seznamům odvolaných certifikátů** .
  - b. Zadejte název seznamu názvů (z kroku [“3.a”](#) na stránce 330) v poli **Seznam názvů CRL** .

#### ***Přístup k značkám CRL a ARL s IBM MQ MQI client***

K dispozici jsou tři možnosti určení serverů LDAP, které obsahují seznamy CRL pro kontrolu pomocí produktu IBM MQ MQI client.

Všimněte si, že v této sekci se informace o seznamech CRL (Certificate Revocation Lists) vztahují také na seznamy odvolaných autorit (ARLs).

Tři způsoby určení serverů LDAP jsou následující:

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




Další podrobnosti naleznete v souvisejících informacích.

Můžete zahrnout až 10 připojení k alternativním serverům LDAP, abyste zajistili nepřetržitost služby, pokud selže jeden nebo více serverů LDAP. Všimněte si, že servery LDAP *musí* obsahovat identické informace.

Nelze přistupovat k seznam CRL LDAP z kanálu produktu IBM MQ MQI client spuštěného na platformě Linux (platforma zSeries).

*Umístění odpovídacího modulu OCSP a serverů LDAP, které obsahují seznamy odvolaných certifikátů (CRL)*  
V systému IBM MQ MQI client můžete zadat umístění odpovídacího modulu OCSP a serverů LDAP (Lightweight Directory Access Protocol), které uchovávají seznamy zrušených certifikátů (CRL).

Tato umístění můžete určit třemi způsoby, zde jsou uvedeny v pořadí klesající priority.  (Pro IBM i viz [Přístup k seznam CRL a ARL na IBM i.](#))

## Když aplikace IBM MQ MQI client vydá volání MQCONN

Můžete určit odpovídací modul OCSP nebo server LDAP, který uchovává seznamy odvolaných certifikátů při volání **MQCONN**.

Na volání příkazu **MQCONN** se struktura voleb připojení MQCNO může odkazovat na strukturu voleb konfigurace SSL, MQSCO. Struktura MQSCO se dále může odkazovat na jednu nebo více struktur záznamů ověřovacích informací, MQAIR. Každá struktura MQAIR obsahuje všechny informace, které produkt IBM MQ MQI client potřebuje pro přístup k odpovídacímu modulu OCSP nebo k serveru LDAP s holdkami CRL. Například jedno z polí ve struktuře MQAIR je adresa URL, na které lze kontaktovat odpovídací modul. Další informace o struktuře MQAIR naleznete v tématu [Záznam aplikace MQAIR-Authentication](#).

## Přístup k odpovídacímu modulu OCSP nebo serverům LDAP pomocí tabulky definic kanálů klienta (ccdt).

Takže produkt IBM MQ MQI client může přistupovat k odpovídacímu modulu OCSP nebo serverům LDAP, které obsahují seznamy CRL, obsahují atributy jednoho nebo více objektů ověřovacích informací v tabulce definic kanálů klienta.

Na správci front serveru můžete definovat jeden nebo více objektů ověřovacích informací. Atributy objektu ověření obsahují všechny informace, které jsou vyžadovány pro přístup k odpovídacímu modulu OCSP (na platformách, kde je protokol OCSP podporován), nebo na serveru LDAP, který obsahuje seznamy odvolaných certifikátů (CRL). Jeden z atributů uvádí adresu URL odpovídacího modulu OCSP, další uvádí adresu hostitele nebo adresu IP systému, na kterém je spuštěn server LDAP.

Objekt ověřovacích informací s typem AUTHTYPE (OCSP) se nepoužívá pro použití ve správcích front IBM i nebo z/OS, ale lze jej zadat na těchto platformách, které mají být zkopírovány do tabulky definic kanálů klienta (CCDT) pro klientské použití.

Chcete-li produktu IBM MQ MQI client povolit přístup k odpovídacímu modulu OCSP nebo serverům LDAP, které obsahují seznamy odvolaných certifikátů, mohou být atributy jednoho nebo více objektů ověřovacích informací zahrnuty do definiční tabulky kanálu klienta. Takové atributy můžete zahrnout do jednoho z následujících způsobů:

### Na platformách serveru AIX, HP-UX, Linux, IBM i, Solarisa Windows

Můžete definovat seznam názvů, který obsahuje názvy jednoho nebo více objektů ověřovacích informací. Poté můžete nastavit atribut správce front **SSLCRLNL** na název tohoto seznamu názvů.

Používáte-li seznamy CRL, může být konfigurován více než jeden server LDAP, aby poskytoval vyšší dostupnost. Záměrem je, aby každý server LDAP udržující stejné seznamy CRL. Pokud je jeden server LDAP nedostupný, když je tento server požadován, může se IBM MQ MQI client pokusit o přístup k jinému.

Atributy objektů ověřovacích informací, které jsou identifikovány v seznamu názvů, jsou souhrnně označovány jako *umístění odvolaných certifikátů*. Když nastavíte atribut správce front **SSLCRLNL** na



název seznamu názvů, bude umístění odvolaných certifikátů (CRL) zkopírováno do tabulky definic kanálů klienta přidružené ke správci front. Pokud lze k tabulce CCDT přistupovat z klientského systému jako sdíleného souboru, nebo pokud je tabulka CCDT poté zkopírována do systému klienta, může produkt IBM MQ MQI client v daném systému používat umístění odvolaných certifikátů v tabulce CCDT k přístupu k odpovídacímu modulu OCSP nebo serverům LDAP, které obsahují seznamy CRL.

Je-li umístění odvolání certifikátu správce front změněno později, změna se projeví v tabulce CCDT přidružené ke správci front. Je-li atribut správce front **SSLCRLNL** nastaven na prázdnou hodnotu, bude umístění odvolaných certifikátů odebráno z tabulky CCDT. Tyto změny se neprojeví v žádné kopii tabulky na klientském systému.

Požadujete-li umístění odvolání certifikátu na straně klienta a serveru pro jiný kanál MQI a správce front serveru se používá k vytvoření umístění odvolaných certifikátů, můžete následujícím způsobem provést následující akce:

1. Na správci front serveru vytvořte umístění odvolaných certifikátů pro použití v systému klienta.
2. Zkopírujte tabulky CCDT obsahující umístění odvolaných certifikátů do systému klienta.
3. Ve správci front serveru změňte umístění odvolání certifikátů na to, co je povinné na serveru kanálu MQI na serveru.
4. Na klientském počítači můžete použít příkaz **runmqsc** s parametrem **-n**.

### Na platformách klienta AIX, HP-UX, Linux, IBM i, Solarisa Windows

CCDT můžete sestavit na klientském počítači pomocí příkazu **runmqsc** s parametry **-n** a **DEFINE AUTHINFO** objekty v souboru CCDT. Pořadí, ve kterém jsou objekty definovány, je pořadí, ve kterém se tyto objekty používají v souboru. Jakýkoliv název, který můžete použít v objektu **DEFINE AUTHINFO**, není uchován v souboru. Při **DISPLAY** objektech **AUTHINFO** v souboru CCDT se používají pouze poziční čísla.

**Poznámka:** Pokud zadáte argument **-n**, nesmíte zadat žádný jiný parametr.

### Použití Active Directory na systému Windows

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 značkám CRL a ARL s IBM MQ classes for Java a IBM MQ classes for JMS***

IBM MQ classes for Java a IBM MQ classes for JMS přistupují k seznamům CRL jinak než na jiných platformách.

Informace o práci s seznamy CRL a ARL pomocí produktu IBM MQ classes for JMS naleznete v tématu [Použití seznamů odvolaných certifikátů](#).

Informace o práci s seznamy CRL a ARL pomocí produktu IBM MQ classes for JMS viz [vlastnost objektu SSLCERTSTORES](#)

### Manipulace s objekty ověřovacích informací

Objekty ověřovacích informací můžete manipulovat pomocí příkazů MQSC nebo PCF, nebo můžete manipulovat s objekty 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 IBM MQ .

Linux

UNIX

V 8.0.0.3

## Použití metody PAM (Pluggable Authentication Method)

Modul PAM lze používat pouze na platformách SYSTÉM UNIX a Linux . Typický systém UNIX má moduly PAM, které implementují tradiční mechanismus ověřování, avšak mohou existovat i další. Stejně jako základní úloha ověření platnosti hesel lze také vyvolat moduly PAM k provedení dalších pravidel.

Konfigurační soubory definují, která metoda ověření má být použita pro každou aplikaci. Příklady aplikací zahrnují standardní přihlášení terminálu, ftp a telnet.

Výhodou modulu PAM je to, že aplikace nemusí vědět o skutečnosti, jak se ID uživatele skutečně ověřuje. Pokud aplikace může poskytovat správný formulář ověřovacích dat na PAM, je tento mechanismus za sebou transparentní.

Forma ověřovacích dat závisí na použitém systému. Například produkt IBM MQ získá heslo prostřednictvím parametrů, jako je struktura [MQCSP](#) použitá ve volání rozhraní API produktu [MQCONN](#) .

**Důležité:** Nemůžete nastavit atribut **AUTHENMD** , dokud nenainstalujete produkt IBM MQ Verze 8.0.0, opravná sada 3, a pak restartujete správce front pomocí **-e CMDLEVEL=úroveň z 802** (v příkazu [strmqm](#) ), abyste nastavili úroveň příkazů, kterou požadujete.

### Konfigurace systému pro použití modulu PAM

Název služby použitý produktem IBM MQ při vyvolání modulu PAM je *ibmmq*.

Všimněte si, že instalace produktu IBM MQ se pokouší zachovat výchozí konfiguraci PAM, která povoluje připojení od uživatelů operačního systému, založená na známých výchozích hodnotách pro různé operační systémy.

Administrátor systému však musí ověřit, zda jsou pravidla definovaná v produktu `/etc/pam.conf` nebo `/etc/pam.d/ibmmq`, soubory stále odpovídající.

## Autorizace přístupu k objektům

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

V systémech SYSTÉM UNIX, Linux a Okna . 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 provedeny při použití zabezpečení v systému, a pokyny pro udělení oprávnění uživatelům k administraci produktu IBM MQ a práci s objekty produktu IBM MQ . Pokud dodané bezpečnostní mechanismy nevyhovují vašim potřebám, můžete vyvinout vlastní uživatelské programy kanálu.

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

Správce oprávnění k objektu (OAM) poskytuje příkazové rozhraní pro udělování a odebrání oprávnění k objektům produktu IBM MQ .

Musíte být vhodně autorizováni pro použití těchto příkazů, jak je popsáno v “Oprávnění k administraci produktu IBM MQ v systémech SYSTÉM UNIX, Linuxu a Okna” na stránce 377. ID uživatele, která jsou autorizována pro administraci produktu IBM MQ , mají oprávnění *superuživatele* ke správci front, což znamená, že jim nemusíte udělit další oprávnění k vydávání jakýchkoli požadavků nebo příkazů MQI.

### Udělení přístupu k objektu IBM MQ v systémech SYSTÉM UNIX, Linuxu a Okna

Pomocí řídicího příkazu **setmqaut** , příkazu **SET AUTHREC** MQSC nebo příkazu **MQCMD\_SET\_AUTH\_REC** PCF udělte přístup k objektům IBM MQ uživatelům a skupinám uživatelů. Všimněte si, že v produktu IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Úplnou definici řídicího příkazu **setmqaut** a jeho syntaxi naleznete v části [setmqaut](#).

Úplnou definici příkazu MQSC **SET AUTHREC** a jeho syntaxi naleznete v části [SET AUTHREC](#).

Úplnou definici příkazu **MQCMD\_SET\_AUTH\_REC** PCF a jeho syntaxi naleznete v tématu [Nastavení záznamu oprávnění](#).

Aby bylo možné použít tento příkaz, musí být spuštěn správce front. Pokud jste změnil přístup pro činitele, změny se projeví okamžitě u OAM.

Chcete-li udělit uživatelům přístup k objektu, je třeba určit:

- Název správce front, který je vlastníkem objektů, se kterými pracujete. Pokud nezadáte název správce front, bude předpokládán výchozí správce front.
- Název a typ objektu (pro jednoznačnou identifikaci objektu). Zadejte název jako *profil* . to je buď explicitní název objektu, nebo generický název včetně zástupných znaků. Podrobný popis generických profilů a použití zástupných znaků v nich viz “[Použití generických profilů OAM na systémech SYSTÉM UNIX, Linuxu a Okna](#)” na stránce 335.
- Jeden nebo více názvů činitelů a skupin, na které se oprávnění vztahuje.

Pokud ID uživatele obsahuje mezery, uzavřete jej do uvozovek, když použijete tento příkaz. V systému Windows můžete kvalifikovat ID uživatele s názvem domény. Pokud skutečné jméno uživatele obsahuje znak zavináč (@), nahraďte jej znakem @@ a zobrazí se, že je součástí ID uživatele, nikoli pomocí oddělovače mezi ID uživatele a názvem domény.

- Seznam autorizací. Každá položka v seznamu uvádí typ přístupu, který má být udělen tomuto objektu (nebo mu bylo odebráno). Každá autorizace v seznamu je uvedena jako klíčové slovo, předpona se znaménkem plus (+) nebo znaménka minus (-). Chcete-li přidat zadané oprávnění, použijte znaménko plus a pomocí znaku minus odeberte autorizaci. Mezi znakem + nebo-znakem a klíčovým slovem nesmí být žádné mezery.

V jednom příkazu můžete zadat libovolný počet autorizací. Například seznam autorizací, které umožňují uživateli nebo skupině vkládat zprávy do fronty a procházet je, ale zrušit přístup k získání zpráv je následující:

```
+browse -get +put
```

### Příklady použití příkazu setmqaut

Následující příklady ukazují 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 groupa a groupb. U systémů SYSTÉM UNIX a Linux tento příkaz také odvolá oprávnění k vložení pro všechny činitele ve stejné primární skupině jako uživatel fvuser.

```
setmqaut -m saturn.queue.manager -t queue -n MyQueue -p fvuser  
-g groupa -g groupb -put
```

## Použití příkazu `setmqaut` s jinou autorizační službou

Pokud používáte vlastní autorizační službu místo OAM, můžete uvést název této služby na příkaz **setmqaut**, abyste přesměřili příkaz na tuto službu. Tento parametr musíte určit, máte-li současně spuštěné více instalovatelných komponent. Pokud tuto aktualizaci nepoužíváte, provede se aktualizace na první instalovatelnou komponentu pro autorizační službu. Ve výchozím nastavení je to dodaný OAM.

## Poznámky k použití příkazu **SET AUTHREC**

Seznam oprávnění pro přidání a seznam oprávnění pro odebrání se nesmí překrývat. Nemůžete například přidat oprávnění pro zobrazení a odebrat oprávnění pro zobrazení v jednom příkazu. Toto pravidlo platí i v případě, že jsou oprávnění vyjádřena různými volbami. Například následující příkaz se nezdaří, protože oprávnění DSP se překrývá s oprávněním ALLADM:

```
SET AUTHREC PROFILE(*) OBJTYPE(Queue) PRINCIPAL(PRINC01) AUTHADD(DSP) AUTHRMV(ALLADM)
```

Výjimkou z tohoto chování je oprávnění ALL. Následující příkaz nejprve přidá oprávnění ALL, a pak odebere oprávnění SETID:

```
SET AUTHREC PROFILE(*) OBJTYPE(Queue) PRINCIPAL(PRINC01) AUTHADD(ALL) AUTHRMV(SETID)
```

Následující příkaz nejprve odebere oprávnění ALL, a pak přidá oprávnění DSP:

```
SET AUTHREC PROFILE(*) OBJTYPE(Queue) PRINCIPAL(PRINC01) AUTHADD(DSP) AUTHRMV(ALL)
```

Bez ohledu na pořadí, v jakém je oprávnění v příkazu zadáno, se oprávnění ALL zpracuje vždy jako první.

## Použití generických profilů OAM na systémech SYSTÉM UNIX, Linuxu a Okna

Generické profily OAM použijte pro nastavení, v rámci jedné operace, oprávnění uživatele pro mnoho objektů; místo toho, abyste museli vydávat samostatné příkazy **setmqaut** nebo příkazy **SET AUTHREC**, proti každému jednotlivému objektu při jeho vytvoření. Všimněte si, že v produktu IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC**.

Použijete-li generické profily v příkazech `setmqaut` nebo `SET AUTHREC`, můžete 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 použitím 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 . 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 dvojité hvězdičky (\*\*) **jednou** v názvu profilu jako:

- Celý název profilu, který odpovídá všem názvům objektů. Pokud například používáte produkt -t p1cs k identifikaci procesů, použijte jako název profilu volbu \*\*, změníte oprávnění pro všechny procesy.
- Jako počáteční, střední nebo koncový kvalifikátor v názvu profilu odpovídá jednomu nebo více kvalifikátorům v názvu objektu. Například, \*\* . ABC identifikuje všechny objekty s konečným kvalifikátorem ABC.

**Poznámka:** Při použití zástupných znaků v systémech SYSTÉM UNIX a Linux **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 použít**. Způsob použití tohoto pravidla je porovnáváním názvů profilů zleva doprava. Kamkoli se liší, negenerický znak je spíše specifický než generický znak. Takže, v tomto příkladu, fronta AB.CD má autoritu **get** (AB.C\* je více specifická než AB. \*).

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

1. ?
2. \*
3. \*\*

## Probíhá výpis nastavení profilu

Úplnou definici řídicího příkazu **dmpmqaut** a jeho syntaxi naleznete v popisu příkazu [dmpmqaute](#).

Úplnou definici příkazu MQSC **DISPLAY AUTHREC** a jeho syntaxi naleznete v příručce [DISPLAY AUTHREC](#).

Úplnou definici příkazu **MQCMD\_INQUIRE\_AUTH\_RECS** PCF a její syntaxi naleznete v tématu [Inquire Authority Records](#).

Následující příklady ukazují použití obslužného příkazu **dmpmqaut** k výpisu záznamů oprávnění pro generické profily:

1. Tento příklad vypíše všechny záznamy oprávnění s profilem, který odpovídá frontě a.b.c pro činitele user1.

```
dmpmqaut -m qm1 -n a.b.c -t q -p user1
```

Výsledný výpis bude vypadat přibližně takto:

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

**Poznámka:** Ačkoli uživatelé produktu SYSTÉM UNIX a 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:** Pouze pro IBM MQ for Windows , všechny zobrazené řídicí služby zahrnují informace o doméně, například:

```
profile:      a.b.*
object type:  queue
entity:       user1@domain1
type:         principal
authority:    get, browse, put, inq
```

### **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 . 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 dvojité hvězdičky (\*\*) **jednou** v názvu profilu jako:

- Celý název profilu, který odpovídá všem názvům objektů. Pokud například používáte produkt -t p1cs k identifikaci procesů, použijte jako název profilu volbu \*\*, změníte oprávnění pro všechny procesy.
- Jako počáteční, střední nebo koncový kvalifikátor v názvu profilu odpovídá jednomu nebo více kvalifikátorům v názvu objektu. Například, \*\* . ABC identifikuje všechny objekty s konečným kvalifikátorem ABC.

**Poznámka:** Při použití zástupných znaků v systémech SYSTÉM UNIX a Linux **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, v tomto příkladu, fronta AB.CD má autoritu **get** (AB.C\* je více specifická než AB. \*).

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

1. ?
2. \*
3. \*\*

Viz [SET AUTHREC](#) pro ekvivalentní informace při použití tohoto příkazu MQSC.

### **Probíhá výpis nastavení profilu**

Chcete-li vypsát aktuální autorizace přidružené k určenému profilu, použijte řídicí příkaz **dmpmqaut**, příkaz MQSC **DISPLAY AUTHREC** nebo příkaz **MQCMD\_INQUIRE\_AUTH\_RECS** PCF. Všimněte si, že v produktu IBM MQ Appliance můžete použít pouze příkaz **DISPLAY AUTHREC**.

Úplnou definici řídicího příkazu **dmpmqaut** a jeho syntaxi naleznete v popisu příkazu [dmpmqaute](#).



Úplnou definici příkazu MQSC **DISPLAY AUTHREC** a jeho syntaxi naleznete v příručce [DISPLAY AUTHREC](#).

Úplnou definici příkazu **MQCMD\_INQUIRE\_AUTH\_RECS** PCF a její syntaxi naleznete v tématu [Inquire Authority Records](#).

Následující příklady ukazují použití obslužného příkazu **dmpmqaut** k výpisu záznamů oprávnění pro generické profily:

1. Tento příklad vypíše všechny záznamy oprávnění s profilem, který odpovídá frontě a.b.c pro činitele user1.

```
dmpmqaut -m qm1 -n a.b.c -t q -p user1
```

Výsledný výpis bude vypadat podobně jako v tomto příkladu:

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

**Poznámka:** Uživatelé SYSTÉM UNIX a Linux nemohou použít volbu -p; místo toho musí použít -g groupname.

2. Tento příklad vypíše všechny záznamy oprávnění s profilem, který odpovídá frontě a.b.c.

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

Výsledný výpis bude vypadat podobně jako v tomto příkladu:

```
profile:      a.b.c
object type:  queue
entity:       Administrator
type:         principal
authority:    all
-----
profile:      a.b.*
object type:  queue
entity:       user1
type:         principal
authority:    get, browse, put, inq
-----
profile:      a.**
object type:  queue
entity:       group1
type:         group
authority:    get
```

3. Tento příklad vypíše všechny záznamy oprávnění pro profil a.b.\*, fronty typu.

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

Výsledný výpis bude vypadat podobně jako v tomto příkladu:

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

4. Tento příklad vypíše všechny záznamy oprávnění pro správce front qmX.

```
dmpmqaut -m qmX
```

Výsledný výpis bude vypadat podobně jako v tomto příkladu:

```

profile:      q1
object type: queue
entity:      Administrator
type:       principal
authority:   all
-----
profile:      q*
object type: queue
entity:      user1
type:       principal
authority:   get, browse
-----
profile:      name.*
object type: namelist
entity:      user2
type:       principal
authority:   get
-----
profile:      pr1
object type: process
entity:      group1
type:       group
authority:   get

```

5. Tento příklad vypíše všechny názvy profilů a typy objektů pro správce front qmX.

```
dmpmqaut -m qmX -l
```

Výsledný výpis bude vypadat podobně jako v tomto příkladu:

```

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

```

**Poznámka:** Pouze pro IBM MQ for Windows , všechny zobrazené řídicí služby zahrnují informace o doméně, například:

```

profile:      a.b.*
object type: queue
entity:      user1@domain1
type:       principal
authority:   get, browse, put, inq

```

## Zobrazení nastavení přístupu

Použijte řídicí příkaz **dspmqaut** , příkaz **DISPLAY AUTHREC** MQSC nebo příkaz **MQCMD\_INQUIRE\_ENTITY\_AUTH** PCF pro zobrazení autorizací, které určitý činitel nebo skupina má pro konkrétní objekt. Všimněte si, že v produktu IBM MQ Appliance můžete použít pouze příkaz **DISPLAY AUTHREC** .

Aby bylo možné použít tento příkaz, musí být spuštěn správce front. Když změníte přístup pro činitele, změny se projeví okamžitě u OAM. Oprávnění lze v daném okamžiku zobrazit pouze pro jednu skupinu nebo činitele.

Úplnou definici řídicího příkazu **dmpmqaut** a jeho syntaxi naleznete v popisu příkazu [dmpmqaute](#).

Úplnou definici příkazu MQSC **DISPLAY AUTHREC** a jeho syntaxi naleznete v příručce [DISPLAY AUTHREC](#).

Úplnou definici příkazu **MQCMD\_INQUIRE\_AUTH\_RECS** PCF a její syntaxi naleznete v tématu [Inquire Authority Records](#).

Následující příklad zobrazuje použití řídicího příkazu **dspmqaut** k zobrazení autorizací, které má skupina GpAdmin k definici procesu s názvem Annuities , která je ve správci front QueueMan1.

```
dspmqaut -m QueueMan1 -t process -n Annuities -g GpAdmin
```

## Změna a zrušení přístupu k objektu IBM MQ

Chcete-li změnit úroveň přístupu, kterou má uživatel nebo skupina k objektu, použijte řídicí příkaz **setmqaut**, příkaz **DELETE AUTHREC** MQSC nebo příkaz **MQCMD\_DELETE\_AUTH\_REC** PCF. Všimněte si, že v produktu IBM MQ Appliance můžete použít pouze příkaz **DELETE AUTHREC**.

Proces odebrání uživatele ze skupiny je popsán v:

- [“Vytvoření a správa skupin v systému Windows”](#) na stránce 113
- [“Vytvoření a správa skupin v systému HP-UX”](#) na stránce 115
- [“Vytvoření a správa skupin v systému AIX”](#) na stránce 116
- [“Vytvoření a správa skupin v systému Solaris”](#) na stránce 118
- [“Vytvoření a správa skupin v systému Linux”](#) na stránce 118

ID uživatele, který vytvoří objekt IBM MQ, má k tomuto objektu přiděleno celé oprávnění k řízení. Odeberete-li toto ID uživatele z lokální skupiny mqm (nebo skupiny administrátorů v systému Windows), nebudou tato oprávnění odvolána. Použijte řídicí příkaz **setmqaut** nebo příkaz **MQCMD\_DELETE\_AUTH\_REC** PCF k odvolání přístupu k objektu pro ID uživatele, který jej vytvořil, poté, co jste jej odebrali ze skupiny mqm nebo Administrátoři.

Úplnou definici příkazu řídicího příkazu **setmqaut** a jeho syntaxi naleznete v části [setmqaut](#).

Úplnou definici příkazu MQSC **DELETE AUTHREC** a jeho syntaxi naleznete v části [DELETE AUTHREC](#).

Úplnou definici příkazu **MQCMD\_DELETE\_AUTH\_REC** PCF a její syntaxi naleznete v tématu [Odstranit záznam oprávnění](#).

V produktu Windows můžete v produktu IBM MQ 8.0 odstranit položky OAM odpovídající konkrétnímu uživatelskému účtu produktu Windows při použití parametru **-u SID** [setmqaut](#).

Prior to IBM MQ 8.0, you had to delete the OAM entries corresponding to a particular Windows user account before deleting the user profile. Nebylo možné odebrat položky OAM po odebrání uživatelského účtu.

## Prevence kontrol přístupu k zabezpečení v systémech Windows, SYSTÉM UNIX a Linux

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):

Informace o důsledcích nastavení proměnné MQSNOAUT a způsobu nastavení MQSNOAUT na platformách Windows a UNIX najdete v tématu [Proměnné prostředí](#).

- Upravte konfigurační soubor správce front a odeberte službu. (Pokud tak učiníte, nemůžete později přidat OAM.)

Pokud používáte **setmqaut** nebo **dspmqaout**, 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.

Je-li objekt OAM odebrán, nelze jej vrátit zpět do existujícího správce front. Důvodem je skutečnost, že OAM musí být na místě vytvoření objektu. Chcete-li znovu použít produkt IBM MQ OAM poté, co byl odebrán, musí být správce front znovu sestaven.

### **Související informace**

[Instalovatelné služby](#)

## **Udělení požadovaného přístupu k prostředkům**

Prostřednictvím tohoto tématu můžete určit, které úlohy mají být provedeny při použití zabezpečení ve vašem systému IBM MQ .

### **Informace o této úloze**

Během této úlohy rozhodujete o tom, jaké akce jsou nezbytné k použití odpovídající úrovně zabezpečení na prvky vaší instalace produktu IBM MQ . Každá jednotlivá úloha, na kterou jste se odkazujete, poskytuje instrukce po krocích pro všechny platformy.

### **Postup**

1. Potřebujete omezit přístup k vašemu správci front některým uživatelům?
  - a) Ne: neprovádět žádnou další akci.
  - b) Ano: Přejděte na další otázku.
2. Potřebují tito uživatelé částečný administrativní přístup k podmnožině prostředků správce front?
  - a) Ne: Přejděte na další otázku.
  - b) Ano: Viz [“Udělení částečného administrativního přístupu k podmnožině prostředků správce front” na stránce 343.](#)
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 352.](#)
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 357.](#)
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 358.](#)
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 360](#)
  - b) Ano: Viz [“Povolení připojení uživatelských aplikací k vašemu správci front” na stránce 360.](#)

## **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 67. 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 <a href="#">“Udělení omezeného administrativního přístupu k některým frontám”</a> na stránce 344 .
Témata	Udělte částečný administrativní přístup k požadovaným tématům, jak je popsáno v tématu <a href="#">“Udělení omezeného administrativního přístupu k některým tématům”</a> na stránce 345 .
Kanály	Udělte částečný administrativní přístup k požadovaným kanálům, jak je popsáno v tématu <a href="#">“Udělení omezeného administrativního přístupu k některým kanálům”</a> na stránce 347 .
Správce front	Udělte částečný administrativní přístup ke správci front, jak je popsáno v tématu <a href="#">“Udělení omezeného administrativního přístupu ke správci front”</a> na stránce 348 .
Procesy	Udělte částečný administrativní přístup k požadovaným procesům, jak je popsáno v tématu <a href="#">“Udělení omezeného administrativního přístupu k některým procesům”</a> na stránce 349 .
Seznamy názvů	Udělení částečného administrativního přístupu k vyžadovaným seznamům názvů, jak je popsáno v tématu <a href="#">“Udělení omezeného administrativního přístupu k některým seznamům názvů”</a> na stránce 350 .
Služby	Udělte částečný administrativní přístup k požadovaným službám, jak je popsáno v tématu <a href="#">“Udělení omezeného administrativního přístupu k některým službám”</a> na stránce 351 .

### 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.


V systémech UNIX, Linux, Windows a IBM můžete také použít příkaz [SET AUTHREC](#) .

**Poznámka:** V produktu IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

#### Procedura

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

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

- 

Pro IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(ReqdAction) MQMNAME(' QMgrName ')
```

-  Pro z/OSzadejte následující příkazy:



```
RDEFINE MQADMIN QMgrName.QUEUE. ObjectProfile UACC(NONE)  
PERMIT QMgrName.QUEUE. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

Tyto příkazy udělují přístup k zadané frontě. Chcete-li určit, které příkazy MQSC může uživatel provést ve frontě, zadejte pro každý příkaz MQSC následující příkazy:

```
RDEFINE MQCMD5 QMgrName. ReqdAction. QType UACC(NONE)  
PERMIT QMgrName. ReqdAction. QType CLASS(MQCMD5) ID(GroupName) ACCESS(ALTER)
```

Chcete-li povolit uživateli použít příkaz DISPLAY QUEUE, zadejte následující příkazy:

```
RDEFINE MQCMD5 QMgrName.DISPLAY. QType UACC(NONE)  
PERMIT QMgrName.DISPLAY. QType CLASS(MQCMD5) ID(GroupName) ACCESS(READ)
```

Názvy proměnných mají následující význam:

#### **QMgrName**

Název správce front. V systému z/OS může být tato hodnota také názvem skupiny sdílení front.

#### **ObjectProfile**



Název objektu nebo generický profil, pro které chcete změnit autorizace.

#### **GroupName**

Název skupiny, ke které má být udělen přístup.

#### **ReqdAction**

Akce, kterou povolujete, aby skupina mohla provést:

- U systémů UNIX, Linux a Windows jsou všechny kombinace následujících autorizací: + chg, + clr, + dlt, + dsp. Oprávnění + alladm je ekvivalentní s + chg + clr + dlt + dsp.
-  V systémech IBM ilibovolná kombinace následujících autorizací: \*ADMCHG, \*ADMCLR, \*ADMDLT, \*ADMDSP. Autorizace \*ALLADM je ekvivalentní ke všem těmito individuálním autorizacím.
-  V systému z/OS jedna z hodnot ALTER, CLEAR, DELETE nebo MOVE.

**Poznámka:** Udělení + crt pro fronty nepřímo činí uživatele nebo skupinu administrátorem. Nepoužívejte oprávnění + crt, abyste udělili omezený administrativní přístup k některým frontám.

#### **QTYPE**

Pro příkaz DISPLAY, jedna z hodnot QUEUE, QLOCAL, QALIAS, QMODEL, QREMOTE nebo QCLUSTER.

Pro jiné hodnoty parametru *ReqdAction*, jedna z hodnot QLOCAL, QALIAS, QMODEL nebo QREMOTE.

### **Udělení omezeného administrativního přístupu k některým tématům**

Udělte přístup k částečnému administrativnímu přístupu k některým tématům ve správci front, a to pro každou skupinu uživatelů, kteří pro ni potřebují obchodní potřeby.

## Informace o této úloze

Chcete-li udělit omezený administrativní přístup k některým tématům pro některé akce, použijte příslušné příkazy pro váš operační systém.

V systémech UNIX, Linux, Windows a IBM můžete také použít příkaz [SET AUTHREC](#) .

**Poznámka:** V produktu IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

## Procedura

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

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

### IBM i

Pro IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*TOPIC) USER(GroupName) AUT(ReqdAction) MQMNAME(' QMgrName ')
```

- z/OS** Pro z/OSzadejte následující příkazy:

**z/OS**

```
RDEFINE MQADMIN QMgrName.TOPIC. ObjectProfile UACC(NONE)  
PERMIT QMgrName.TOPIC. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

Tyto příkazy udělují přístup k uvedenému tématu. Chcete-li určit, které příkazy MQSC může uživatel provést na daném tématu, zadejte pro každý příkaz MQSC následující příkazy:

```
RDEFINE MQCMDS QMgrName. ReqdAction.TOPIC UACC(NONE)  
PERMIT QMgrName. ReqdAction.TOPIC CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
```

Chcete-li povolit uživateli použít příkaz DISPLAY TOPIC, zadejte následující příkazy:

```
RDEFINE MQCMDS QMgrName.DISPLAY.TOPIC UACC(NONE)  
PERMIT QMgrName.DISPLAY.TOPIC CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

Názvy proměnných mají následující význam:

### QMGrName

Název správce front. **z/OS** V systému z/OS může být tato hodnota také názvem skupiny sdílení front.

### ObjectProfile

Název objektu nebo generický profil, pro které chcete změnit autorizace.

### GroupName

Název skupiny, ke které má být udělen přístup.

### ReqdAction

Akce, kterou povolujete, aby skupina mohla provést:

- V systémech UNIX, Linux a Windows jsou všechny kombinace následujících autorizací: + chg, + clr, + crt, + dlt, + dsp. + CTRL. Oprávnění + alladm je ekvivalentní s + chg + clr + dlt + dsp.
- **IBM i** V systému IBM ilibovolná kombinace následujících autorizací: \*ADMCHG, \*ADMCLR, \*ADMCRRT, \*ADMCLT, \*ADMDSPL, \*CTRL. Autorizace \*ALLADM je ekvivalentní ke všem těmito individuálními autorizacím.
- **z/OS** V systému z/OS jedna z hodnot ALTER, CLEAR, DEFINE, DELETE nebo MOVE.

## Udělení omezeného administrativního přístupu k některým kanálům

Udělte některým kanálům ve správci front částečný administrativní přístup k některým kanálům, a to pro každou skupinu uživatelů, kteří pro ni budou potřebovat obchodní položku.

### Informace o této úloze

Chcete-li některým kanálům pro některé akce udělit omezený administrativní přístup k některým kanálům, použijte příslušné příkazy pro daný operační systém.

V systémech UNIX, Linux, Windows a IBM můžete také použít příkaz [SET AUTHREC](#).

**Poznámka:** V produktu IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC**.

### Procedura

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

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

- IBM i**

Pro IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*CHL) USER(GroupName) AUT(ReqdAction) MQMNAME(' QMgrName ')
```

- z/OS** Pro z/OSzadejte následující příkazy:

- z/OS**

```
RDEFINE MQADMIN QMgrName.CHANNEL. ObjectProfile UACC(NONE)  
PERMIT QMgrName.CHANNEL. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

Tyto příkazy udělují přístup k uvedenému kanálu. Chcete-li určit, které příkazy MQSC může uživatel na kanálu provést, zadejte pro každý příkaz MQSC následující příkazy:

```
RDEFINE MQCMDS QMgrName. ReqdAction.CHANNEL UACC(NONE)  
PERMIT QMgrName. ReqdAction.CHANNEL CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
```

Chcete-li povolit uživateli použít příkaz DISPLAY CHANNEL, zadejte následující příkazy:

```
RDEFINE MQCMDS QMgrName.DISPLAY.CHANNEL UACC(NONE)  
PERMIT QMgrName.DISPLAY.CHANNEL CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

Názvy proměnných mají následující význam:

#### QMgrName

Název správce front. V systému z/OS může být tato hodnota také názvem skupiny sdílení front.

#### ObjectProfile

Název objektu nebo generický profil, pro které chcete změnit autorizace.

#### GroupName

Název skupiny, ke které má být udělen přístup.

#### ReqdAction

Akce, kterou povolujete, aby skupina mohla provést:

- V systémech UNIX, Linux a Windows jsou všechny kombinace následujících autorizací: + chg, + clr, + crt, + dlt, + dsp. + ctrl, + ctrlx. Oprávnění + alladm je ekvivalentní s + chg + clr + dlt + dsp.



- **IBM i** V systémech IBM ilibovolná kombinace následujících autorizací: \*ADMCHG, \*ADMCLR, \*ADMCRRT, \*ADMDLT, \*ADMDSP, \*CTRL, \*CTRLx. Autorizace \*ALLADM je ekvivalentní ke všem těmto individuálním autorizacím.
- **z/OS** V systému z/OSjedna z hodnot ALTER, CLEAR, DEFINE, DELETE nebo MOVE.

### **Udělení omezeného administrativního přístupu ke správci front**

Udělte přístup k částečnému administrativnímu přístupu ke správci front, do každé skupiny uživatelů, kteří pro ni potřebují obchodní potřeby.

#### **Informace o této úloze**

Chcete-li udělit omezený administrativní přístup k provádění některých akcí ve správci front, použijte příslušné příkazy pro daný operační systém.

V systémech UNIX, Linux, Windows a IBM imůžete také použít příkaz [SET AUTHREC](#) .

**Poznámka:** V produktu IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

#### **Procedura**

- Pro systémy UNIX, Linux a Windows zadejte následující 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 MQCMD5 QMgrName.ReqdAction.QMGR UACC(NONE)
PERMIT QMgrName.ReqdAction.QMGR CLASS(MQCMD5) ID(GroupName) ACCESS(ALTER)
```

Chcete-li povolit uživateli použít příkaz DISPLAY QMGR, zadejte následující příkazy:

```
RDEFINE MQCMD5 QMgrName.DISPLAY.QMGR UACC(NONE)
PERMIT QMgrName.DISPLAY.QMGR CLASS(MQCMD5) 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 jsou všechny kombinace následujících autorizací: + chg, + clr, + crt, + dlt, + dsp. Oprávnění + alladm je ekvivalentní s + chg + clr + dlt + dsp.

Ačkoli + set je autorizace MQI a není obvykle považována za administrativně, může udělení + nastavení ve správci front nepřímo vést k úplnému administrativnímu oprávnění. Nepřidělovat + nastavit běžným uživatelům a aplikacím.

- ▶ **IBM i** V systémech IBM ilibovolná kombinace následujících autorizací: \*ADMCHG, \*ADMCLR, \*ADMCR, \*ADMCLT, \*ADMDS. Autorizace \*ALLADM je ekvivalentní ke všem těmto individuálním autorizacím.

### **Udělení omezeného administrativního přístupu k některým procesům**

Udělte některým procesům ve správci front částečný administrativní přístup k některým procesům, a to pro každou skupinu uživatelů, kteří pro ni potřebují obchodní potřeby.

### **Informace o této úloze**

Chcete-li u některých akcí udělit omezený administrativní přístup k některým procesům, použijte příslušné příkazy pro daný operační systém.

V systémech UNIX, Linux, Windows a IBM můžete také použít příkaz [SET AUTHREC](#) .

**Poznámka:** V produktu IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

### **Procedura**

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

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

- ▶ **IBM i**

Pro IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*PRC) USER(GroupName) AUT(ReqdAction) MQMNAME(' QMgrName ')
```

- ▶ **z/OS** Pro z/OSzadejte následující příkazy:

▶ **z/OS**

```
RDEFINE MQADMIN QMgrName.PROCESS. ObjectProfile UACC(NONE)  
PERMIT QMgrName.PROCESS. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

Tyto příkazy udělují přístup k uvedenému kanálu. Chcete-li určit, které příkazy MQSC může uživatel na kanálu provést, zadejte pro každý příkaz MQSC následující příkazy:

```
RDEFINE MQCMDS QMgrName. ReqdAction.PROCESS UACC(NONE)  
PERMIT QMgrName. ReqdAction.PROCESS CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
```

Chcete-li povolit uživateli použít příkaz DISPLAY PROCESS, zadejte následující příkazy:

```
RDEFINE MQCMDS QMgrName.DISPLAY.PROCESS UACC(NONE)  
PERMIT QMgrName.DISPLAY.PROCESS CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

Názvy proměnných mají následující význam:

#### **QMGrName**

Název správce front. ▶ **z/OS** V systému z/OS může být tato hodnota také názvem skupiny sdílení front.

#### **ObjectProfile**



Název objektu nebo generický profil, pro které chcete změnit autorizace.

## GroupName

Název skupiny, ke které má být udělen přístup.

## ReqdAction

Akce, kterou povolujete, aby skupina mohla provést:

- V systémech UNIX, Linux a Windows jsou všechny kombinace následujících autorizací: + chg, + clr, + crt, + dlt, + dsp. Oprávnění + alladm je ekvivalentní s + chg + clr + dlt + dsp.
-  V systémech IBM libovolná kombinace následujících autorizací: \*ADMCHG, \*ADMCLR, \*ADMCRRT, \*ADMCLT, \*ADMCLD, \*ADMCLP. Autorizace \*ALLADM je ekvivalentní ke všem těmto individuálním autorizacím.
-  V systému z/OS jedna z hodnot ALTER, CLEAR, DEFINE, DELETE nebo MOVE.

## Udělení omezeného administrativního přístupu k některým seznamům názvů

Udělte některým seznamům názvů ve správci front částečný administrativní přístup k některým seznamům názvů, a to pro každou skupinu uživatelů, kteří pro ni potřebují obchodní potřeby.

## Informace o této úloze

Chcete-li udělit omezený administrativní přístup k některým seznamům názvů pro některé akce, použijte příslušné příkazy pro váš operační systém.

V systémech UNIX, Linux, Windows a IBM můžete také použít příkaz [SET AUTHREC](#).

**Poznámka:** V produktu IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC**.

## Procedura

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


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


- 


Pro IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*NMLIST) USER(GroupName) AUT(ReqdAction) MQMNAME(' QMgrName ')
```


-  Pro z/OSzadejte následující příkazy:

```
 RDEFINE MQADMIN QMgrName.NAMELIST. ObjectProfile UACC(NONE)  
PERMIT QMgrName.NAMELIST. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

 Tyto příkazy udělují přístup k uvedenému seznamu názvů. Chcete-li určit, které příkazy MQSC může uživatel v daném seznamu názvů provést, zadejte pro každý příkaz MQSC následující příkazy:

```
 RDEFINE MQCMDS QMgrName. ReqdAction.NAMELIST UACC(NONE)  
PERMIT QMgrName. ReqdAction.NAMELIST CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
```

 Chcete-li povolit uživateli použít příkaz DISPLAY NAMELIST, zadejte následující příkazy:

```
 RDEFINE MQCMDS QMgrName.DISPLAY.NAMELIST UACC(NONE)  
PERMIT QMgrName.DISPLAY.NAMELIST CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

Názvy proměnných mají následující význam:



**QMgrName**

Název správce front.

**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 jsou všechny kombinace následujících autorizací: + chg, + clr, + crt, + dlt, + ctrl, + ctrlx, + dsp. Oprávnění + alladm je ekvivalentní s + chg + clr + dlt + dsp.
-  V systémech IBM ilibovolná kombinace následujících autorizací: \*ADMCHG, \*ADMCLR, \*ADMCRRT, \*ADMCLT, \*ADM DSP, \*CTRL, \*CTRLX. Autorizace \*ALLADM je ekvivalentní ke všem těmto individuálním autorizacím.

## Udělení úplného administrativního přístupu k podmnožině prostředků správce front

Je třeba, abyste určitým uživatelům poskytli úplný administrativní přístup k některým prostředkům správce front, ale ne ke všem prostředkům správce front. Použijte tyto tabulky k určení akcí, které musíte provést.

<i>Tabulka 68. Udělení úplného administrativního přístupu k podmnožině prostředků správce front</i>	
<b>Uživatelé potřebují spravovat objekty tohoto typu</b>	<b>Provést tuto akci</b>
Fronty	Udělte úplný administrativní přístup k požadovaným frontám, jak je popsáno v tématu <a href="#">“Udělení úplného administrativního přístupu k některým frontám”</a> na stránce 353 .
Témata	Udělte úplný administrativní přístup k požadovaným tématům, jak je popsáno v tématu <a href="#">“Udělení úplného administrativního přístupu k některým tématům”</a> na stránce 353 .
Kanály	Udělte úplný administrativní přístup k požadovaným kanálům, jak je popsáno v tématu <a href="#">“Udělení úplného administrativního přístupu k některým kanálům”</a> na stránce 354 .
Správce front	Udělte úplný administrativní přístup ke správci front, jak je popsáno v tématu <a href="#">“Udělení úplného administrativního přístupu ke správci front”</a> na stránce 355 .
Procesy	Udělte úplný administrativní přístup k požadovaným procesům, jak je popsáno v tématu <a href="#">“Udělení úplného administrativního přístupu k některým procesům”</a> na stránce 355 .
Seznamy názvů	Udělit úplný administrativní přístup k vyžadovaným seznamům názvů, jak je popsáno v tématu <a href="#">“Udělení úplného administrativního přístupu k některým seznamům názvů”</a> na stránce 356

Tabulka 68. Udělení úplného administrativního přístupu k podmnožině prostředků správce front (pokračování)

Uživatelé potřebují spravovat objekty tohoto typu	Provést tuto akci
Služby	Udělte úplný administrativní přístup k požadovaným službám, jak je popsáno v tématu <a href="#">“Udělení úplného administrativního přístupu k některým službám”</a> na stránce 357

### **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.

V systémech UNIX, Linux, Windows a IBM můžete také použít příkaz [SET AUTHREC](#) .

**Poznámka:** V produktu IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

#### **Procedura**

- Pro systémy UNIX, Linux a Windows zadejte následující 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 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 být tato hodnota také názvem skupiny sdílení front.

#### **ObjectProfile**

Název objektu nebo generický profil, pro které chcete změnit autorizace.

#### **GroupName**

Název skupiny, ke které má být udělen přístup.

### **Udělení úplného administrativního přístupu k některým tématům**

Udělte úplný administrativní přístup k některým tématům ve správci front, do každé skupiny uživatelů, kteří pro ni potřebují obchodní potřeby.

#### **Informace o této úloze**

Chcete-li udělit úplný administrativní přístup k některým tématům pro některé akce, použijte příslušné příkazy pro váš operační systém.

V systémech UNIX, Linux, Windows a IBM můžete také použít příkaz [SET AUTHREC](#) .

**Poznámka:** V produktu IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

## Procedura

- Pro systémy UNIX, Linux a Windows zadejte následující 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 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/OS může být tato hodnota také názvem skupiny sdílení front.

### **ObjectProfile**

Název objektu nebo generický profil, pro které chcete změnit autorizace.

### **GroupName**

Název skupiny, ke které má být udělen přístup.

## ***Udělení úplného administrativního přístupu k některým kanálům***

Udělte úplný administrativní přístup k některým kanálům ve správci front, a to pro každou skupinu uživatelů, kteří pro ni potřebují obchodní činnost.

## **Informace o této úloze**

Chcete-li udělit úplný administrativní přístup k některým kanálům, použijte příslušné příkazy pro daný operační systém.

V systémech UNIX, Linux, Windows a IBM můžete také použít příkaz [SET AUTHREC](#) .

**Poznámka:** V produktu IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

## Procedura

- Pro systémy UNIX, Linux a Windows zadejte následující 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 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/OS může být tato hodnota také názvem skupiny sdílení front.

### **ObjectProfile**

Název objektu nebo generický profil, pro které chcete změnit autorizace.

### GroupName

Název skupiny, ke které má být udělen přístup.

### **Udělení úplného administrativního přístupu ke správci front**

Udělte úplný administrativní přístup ke správci front, do každé skupiny uživatelů, kteří pro ni potřebují obchodní potřeby.

### **Informace o této úloze**

Chcete-li udělit úplný administrativní přístup ke správci front, použijte příslušné příkazy pro váš operační systém.

V systémech UNIX, Linux, Windows a IBM můžete také použít příkaz [SET AUTHREC](#) .

**Poznámka:** V produktu IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

### **Procedura**

- Pro systémy UNIX, Linux a Windows zadejte následující 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 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 být tato hodnota také názvem skupiny sdílení front.

#### **ObjectProfile**

Název objektu nebo generický profil, pro které chcete změnit autorizace.

#### **GroupName**

Název skupiny, ke které má být udělen přístup.

### **Udělení úplného administrativního přístupu k některým procesům**

Udělte úplný administrativní přístup k některým procesům ve správci front, a to pro každou skupinu uživatelů, kteří pro ni potřebují obchodní činnost.

### **Informace o této úloze**

Chcete-li udělit úplný administrativní přístup k některým procesům, použijte příslušné příkazy pro váš operační systém.

V systémech UNIX, Linux, Windows a IBM můžete také použít příkaz [SET AUTHREC](#) .

**Poznámka:** V produktu IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

### **Procedura**

- Pro systémy UNIX, Linux a Windows zadejte následující 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 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/OS může být tato hodnota také názvem skupiny sdílení front.

#### **ObjectProfile**

Název objektu nebo generický profil, pro které chcete změnit autorizace.

#### **GroupName**

Název skupiny, ke které má být udělen přístup.

### ***Udělení úplného administrativního přístupu k některým seznamům názvů***

Udělte úplný administrativní přístup k některým seznamům názvů ve správcí 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.

V systémech UNIX, Linux, Windows a IBM můžete také použít příkaz [SET AUTHREC](#) .

**Poznámka:** V produktu IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

### **Procedura**

- Pro systémy UNIX, Linux a Windows zadejte následující 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 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/OS může být tato hodnota také názvem skupiny sdílení front.

#### **ObjectProfile**

Název objektu nebo generický profil, pro které chcete změnit autorizace.

#### **GroupName**

Název skupiny, ke které má být udělen přístup.

## Udělení úplného administrativního přístupu k některým službám

Udělte úplný administrativní přístup k některým službám ve správci front, do každé skupiny uživatelů, kteří pro ni potřebují obchodní potřeby.

### Informace o této úloze

Chcete-li udělit úplný administrativní přístup k některým službám, použijte příslušné příkazy pro váš operační systém.

V systémech UNIX, Linux, Windows a IBM můžete také použít příkaz [SET AUTHREC](#) .

**Poznámka:** V produktu IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

### Procedura

- Pro systémy UNIX, Linux a Windows zadejte následující 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 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 být tato hodnota také názvem skupiny sdílení front.

#### **ObjectProfile**

Název objektu nebo generický profil, pro které chcete změnit autorizace.

#### **GroupName**

Název skupiny, ke které má být udělen přístup.

## Udělení přístupu 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.

V systémech UNIX, Linux, Windows a IBM můžete také použít příkaz [SET AUTHREC](#) .

**Poznámka:** V produktu IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

Po provedení změn všech podrobností autorizace provedte aktualizaci zabezpečení pomocí příkazu [REFRESH SECURITY](#) .

### Procedura

- Pomocí průvodce:
  - a) V podokně Navigator produktu IBM MQ Explorer 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 MQ Explorer.

- Pro IBM izadejte následující příkazy:

```
GRTMQMAUT OBJ(*ALL) OBJTYPE(*Q) USER('GroupName') AUT(*ADM DSP *BROWSE) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*TOPIC) USER('GroupName') AUT(*ADM DSP) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*CHL) USER('GroupName') AUT(*ADM DSP *INQ) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*CLTCN) USER('GroupName') AUT(*ADM DSP) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*AUTHINFO) USER('GroupName') AUT(*ADM DSP) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*LSR) USER('GroupName') AUT(*ADM DSP) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*NMLIST) USER('GroupName') AUT(*ADM DSP) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*PRC) USER('GroupName') AUT(*ADM DSP) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*SVC) USER('GroupName') AUT(*ADM DSP) MQMNAME('QMgrName')
GRTMQMAUT OBJ('object-name') OBJTYPE(*MQM) USER('GroupName') AUT(*ADM DSP *CONNECT *INQ)
MQMNAME('QMgrName')
```

- Pro z/OSzadejte následující příkazy:

```
RDEFINE MQQUEUE QMgrName.** UACC(NONE)
PERMIT QMgrName.** CLASS(MQQUEUE) ID(GroupName) ACCESS(READ)
RDEFINE MXTOPIC QMgrName.** UACC(NONE)
PERMIT QMgrName.** CLASS(MXTOPIC) ID(GroupName) ACCESS(READ)
RDEFINE MQPROC QMgrName.** UACC(NONE)
PERMIT QMgrName.** CLASS(MQPROC) ID(GroupName) ACCESS(READ)
RDEFINE MQNLIST QMgrName.** UACC(NONE)
PERMIT QMgrName.** CLASS(MQNLIST) ID(GroupName) ACCESS(READ)
RDEFINE MQCONN QMgrName.BATCH UACC(NONE)
PERMIT QMgrName.BATCH CLASS(MQCONN) ID(GroupName) ACCESS(READ)
RDEFINE MQCONN QMgrName.CICS UACC(NONE)
PERMIT QMgrName.CICS CLASS(MQCONN) ID(GroupName) ACCESS(READ)
RDEFINE MQCONN QMgrName.IMS UACC(NONE)
PERMIT QMgrName.IMS CLASS(MQCONN) ID(GroupName) ACCESS(READ)
RDEFINE MQCONN QMgrName.CHIN UACC(NONE)
PERMIT QMgrName.CHIN CLASS(MQCONN) ID(GroupName) ACCESS(READ)
```

Názvy proměnných mají následující význam:

#### **QMgrName**

Název správce front. V systému z/OS může být tato hodnota také názvem 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**

Můžete použít průvodce Přidat oprávnění založená na rolích nebo příslušné příkazy pro váš operační systém.

V systémech UNIX, Linux, Windows a IBM můžete také použít příkaz `SET AUTHREC` .

**Poznámka:** V produktu IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

#### Notes:

1. Používáte-li produkt **runmqsc** k administraci správce front místo produktu MQ Explorer, musíte udělit oprávnění k dotazům, získání a procházení `SYSTEM.MQSC.REPLY.QUEUE` a vy nemusíte udělovat žádné oprávnění k `SYSTEM.MQEXPLORER.REPLY.MODEL` fronta.
2. Při poskytnutí přístupu uživatele ke všem prostředkům ve správci front existují některé příkazy, které uživatel nemůže spustit, pokud tento uživatel nemá přístup pro čtení k souboru `qm.ini` . Důvodem je omezení na to, aby uživatelé produktu mqm , kteří nejsou schopni číst soubor `qm.ini` , byli schopni číst.

Uživatel nemůže vydat následující příkazy, pokud jste tomuto uživateli neudělili přístup pro čtení k souboru `qm.ini` :

- Definování kanálu, který je konfigurován pro použití TLS
- Definování kanálu pomocí proměnných vložení s automatickou konfigurací, které jsou definovány v produktu `qm.ini`

## Procedura

- Pokud používáte průvodce, klepněte v podokně Navigator produktu IBM MQ Explorer pravým tlačítkem myši na správce front a poté klepněte na volbu **Oprávnění pro objekty > Přidat oprávnění založená na rolích**.

Otevře se průvodce Přidat oprávnění založená na rolích.

-  

Pro systémy SYSTÉM UNIX a 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 SYSTÉM UNIX a 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 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/OS může být tato hodnota také názvem skupiny sdílení front.

**GroupName**

Název skupiny, ke které má být udělen přístup.

## Odebrání konektivity ke správci front

Pokud nechcete, aby se uživatelské aplikace připojovaly k vašemu správci front, odeberte jejich oprávnění pro připojení k tomuto správci front.

### Informace o této úloze

Odvolejte oprávnění všech uživatelů pro připojení ke správci front pomocí příslušného příkazu pro váš operační systém.

V systémech UNIX, Linux, Windows a IBM můžete také použít příkaz `DELETE AUTHREC`.

**Poznámka:** V produktu IBM MQ Appliance můžete použít pouze příkaz **DELETE AUTHREC**.

### Procedura

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

```
setmqaut -m QMgrName -t qmgr -g GroupName -connect
```

- Pro IBM izadejte tento příkaz:

```
RVKMQMAUT OBJ (' QMgrName ') OBJTYPE(*MQM) USER(*ALL) AUT(*CONNECT)
```

- Pro z/OS zadejte 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/OS může být tato hodnota také názvem skupiny sdílení front.

**GroupName**

Název skupiny, kterému má být odepřen přístup.

## Povolení připojení uživatelských aplikací k vašemu správci front

Chcete povolit uživatelům aplikace připojit se k vašemu správci front. Použijte tabulky uvedené v tomto tématu k určení akcí, které mají být provedeny.

Nejprve určete, zda se klientské aplikace budou připojovat ke správci front.

Pokud žádná z aplikací, které se nebudou připojovat k vašemu správci front, jsou klientské aplikace, zakažte vzdálený přístup, jak je popsáno v tématu [“Zakázání vzdáleného přístupu ke správci front”](#) na stránce 368.

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 361.

V obou případech nastavte zabezpečení připojení podle popisu v části [“Nastavení zabezpečení připojení”](#) na stránce 368.

Chcete-li řídit přístup k prostředkům pro každého uživatele připojícího se ke správci front, prohlédněte si následující tabulku. Je-li příkaz v prvním sloupci true, proveďte akci uvedenou ve druhém sloupci.

<b>Příkaz</b>	<b>Provést tuto akci</b>
Máte aplikace, které využívají fronty.	Viz <a href="#">“Řízení uživatelského přístupu k frontám”</a> na stránce 369
Máte aplikace, které využívají témata	Viz <a href="#">“Řízení přístupu uživatelů k tématům”</a> na stránce 374.
Máte aplikace, které se dotazujete na objekt správce front	Viz <a href="#">“Udělení oprávnění k dotazům na správce front”</a> na stránce 375.
Máte aplikace, které používají objekty procesu	Viz <a href="#">“Udělení oprávnění pro přístup k procesům”</a> na stránce 376
Máte aplikace, které používají seznamy názvů	Viz <a href="#">“Udělení oprávnění pro přístup k seznamům názvů”</a> na stránce 377

### **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**

- Použití SSL nebo TLS se záznamy ověření kanálu:
  - Zabraňte jakémukoliv Distinguished Name (DN) z otevření kanálu tak, že použijete záznam ověření kanálu SSLPEERMAP k mapování všech DN na USERSRC (NOACCESS).
  - Povolit specifickým jménům DN nebo sad DN pro otevření kanálu pomocí záznamu ověřování kanálu SSLPEERMAP, který je namapuje na USERSRC (CHANNEL).
- Použití SSL nebo TLS s uživatelskou procedurou zabezpečení:
  - Nastavte hodnotu MCAUSER na kanálu připojení serveru na identifikátor uživatele bez oprávnění.
  - 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.
- Použití SSL nebo TLS s hodnotami definice pevného kanálu:
  - Nastavte parametr SSLPEER na kanál připojení serveru na specifickou hodnotu nebo zúžnou škálu hodnot.
  - Nastavte MCAUSER na kanál připojení serveru na ID uživatele, se kterým má být kanál spuštěn.
- Použití záznamů ověření kanálu u kanálů, které nepoužívají SSL nebo TLS:
  - Zabraňte jakýmkoli IP adresám z otevíracích kanálů pomocí záznamu ověřování kanálu mapování adres s parametrem ADDRESS (\*) a USERSRC (NOACCESS).
  - Povolit použití určitých adres IP pro otevírání kanálů pomocí ověřovacích záznamů kanálu mapování adres pro tyto adresy s USERSRC (CHANNEL).
- Použití uživatelské procedury zabezpečení:
  - Napište proceduru zabezpečení k autorizaci připojení na základě libovolné vlastnosti, kterou vyberete, například z původní adresy IP.
- 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 informace

[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 362](#)

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 informace

[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 uživateli naleznete v tématu "Oprávnění uživatelé" na stránce 318. Další informace o příkazu \*MQADMIN naleznete v části [SET CHLAUTH](#).

## Související informace

### [SET CHLAUTH](#)

*Mapování vzdáleného správce front na ID uživatele MCAUSER*

K nastavení atributu MCAUSER kanálu podle správce front, ze kterého se kanál připojuje, můžete použít záznam ověření kanálu.

## Než začnete

Ujistěte se, že jsou záznamy ověření kanálu povoleny následujícím způsobem:

```
ALTER QMGR CHLAUTH(ENABLED)
```

## Informace o této úloze

Volitelně můžete omezit adresy IP, na které se pravidlo vztahuje.

Všimněte si, že tato technika se nevztahuje na kanály připojení serveru. Uvedete-li název kanálu připojení serveru v následujících příkazech, nebude mít žádný účinek.

## Procedura

- Nastavte záznam ověřování kanálu pomocí příkazu MQSC **SET CHLAUTH** nebo příkazu PCF **Set Channel Authentication Record**. Můžete například zadat příkaz MQSC:

```
SET CHLAUTH(' generic-channel-name ') TYPE (QMGRMAP) QMNAME(generic-partner-qmgr-name ) USERSRC(MAP) MCAUSER(user)
```

*generic-channel-name* je název kanálu, ke kterému chcete řídit přístup, nebo vzor obsahující symbol hvězdičky (\*) jako zástupný znak, který odpovídá názvu kanálu.

*generický-partner-qmgr-name* je buď název správce front, nebo vzor obsahující symbol hvězdičky (\*) jako zástupný znak, který odpovídá názvu správce front.

*uživatel* je ID uživatele, které má být použito pro všechna připojení z uvedeného správce front.

- Chcete-li omezit tento příkaz na určité IP adresy, začleňte parametr **ADDRESS** následujícím způsobem:

```
SET CHLAUTH(' generic-channel-name ') TYPE (QMGRMAP) QMNAME(generic-partner-qmgr-name ) USERSRC(MAP) MCAUSER(user) ADDRESS( generic-ip-address)
```

*generic-channel-name* je název kanálu, ke kterému chcete řídit přístup, nebo vzor obsahující symbol hvězdičky (\*) jako zástupný znak, který odpovídá názvu kanálu.

*generická-adresa-ip* je buď jednotlivá adresa, nebo vzor obsahující symbol hvězdičky (\*) jako zástupný znak nebo znak pomlčky (-), který určuje rozsah, který odpovídá adrese. Další informace o generických adresách IP najdete v tématu [Generické IP adresy](#).

## Související informace

### [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 informace

[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) SSLCERTI(generic-issuer-name)
USERSRC(MAP) MCAUSER(user)
```

*generic-channel-name* je název kanálu, ke kterému chcete řídit přístup, nebo vzor obsahující symbol hvězdičky (\*) jako zástupný znak, který odpovídá názvu kanálu.

*generic-ssl-peer-name* je řetězec následující za standardními pravidly IBM MQ pro hodnoty SSLPEER. Viz IBM MQ pravidla pro hodnoty SSLPEER.

*uživatel* je ID uživatele, které má být použito pro všechna připojení používající zadané DN.

*generický-vydavatel-název* odkazuje na DN vydávajícího certifikátu, který má odpovídat. Tento parametr je volitelný, ale měli byste jej použít, abyste se vyhnuli chybnému porovnávání chybného certifikátu, pokud se používá více certifikačních autorit.

## Související informace

[SET CHLAUTH](#)

*Blokování přístupu ze vzdáleného správce front*

Záznam ověření kanálu můžete použít, chcete-li vzdálenému správci front zabránit v spouštění kanálů.

## Než začnete

Ujistěte se, že jsou záznamy ověření kanálu povoleny následujícím způsobem:

```
ALTER QMGR CHLAUTH(ENABLED)
```

## Informace o této úloze

Všimněte si, že tato technika se nevztahuje na kanály připojení serveru. Zadáte-li v následujícím příkazu název kanálu připojení serveru, nebude mít žádný účinek.

## Postup

Nastavte záznam ověřování kanálu pomocí příkazu MQSC **SET CHLAUTH** nebo příkazu PCF **Set Channel Authentication Record**. Můžete například zadat příkaz MQSC:

```
SET CHLAUTH(' generic-channel-name ') TYPE(QMGRMAP) QMNAME(' generic-partner-qmgr-name ')  
USERSRC(NOACCESS)
```

*generic-channel-name* je název kanálu, ke kterému chcete řídit přístup, nebo vzor obsahující symbol hvězdičky (\*) jako zástupný znak, který odpovídá názvu kanálu.

*generický-partner-qmgr-name* je buď název správce front, nebo vzor obsahující symbol hvězdičky (\*) jako zástupný znak, který odpovídá názvu správce front.

## Související informace

[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 informace

[SET CHLAUTH](#)

## Blokování přístupu pro rozlišující název SSL

Můžete použít záznam ověření kanálu, abyste zabránili Rozlišujícímu názvu (DN) SSL ze spuštění kanálů.

### Než začnete

Ujistěte se, že jsou záznamy ověření kanálu povoleny následujícím způsobem:

```
ALTER QMGR CHLAUTH(ENABLED)
```

### Postup

Nastavte záznam ověřování kanálu pomocí příkazu MQSC **SET CHLAUTH** nebo příkazu PCF **Set Channel Authentication Record**. Můžete například zadat příkaz MQSC:

```
SET CHLAUTH('generic-channel-name') TYPE(SSLPEERMAP)  
SSLPEER('generic-ssl-peer-name') SSLCERTI(generic-issuer-name)  
USERSRC(NOACCESS)
```

*generic-channel-name* je název kanálu, ke kterému chcete řídit přístup, nebo vzor obsahující symbol hvězdičky (\*) jako zástupný znak, který odpovídá názvu kanálu.

*generic-ssl-peer-name* je řetězec následující za standardními pravidly IBM MQ pro hodnoty SSLPEER. Viz IBM MQ pravidla pro hodnoty SSLPEER.

*generický-vydavatel-název* odkazuje na DN vydávajícího certifikátu, který má odpovídat. Tento parametr je volitelný, ale měli byste jej použít, abyste se vyhnuli chybnému porovnávání chybného certifikátu, pokud se používá více certifikačních autorit.

### Související informace

[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 informace

[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.

V systémech UNIX, Linux, Windows a IBM můžete také použít příkaz [SET AUTHREC](#).

**Poznámka:** V produktu IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC**.

### Procedura

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

```
setmqaut -m QMgrName -t qmgr -g GroupName +connect
```

- Pro IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ('QMgrName') OBJTYPE(*MQM) USER('GroupName') AUT(*CONNECT)
```

- Pro 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 dávce, CICS, IMS a inicializátoru kanálu (CHIN). Pokud nepoužíváte konkrétní typ připojení, vynechte příslušné příkazy.

Názvy proměnných mají následující význam:

#### QMgrName

Název správce front. V systému z/OS může být tato hodnota také názvem skupiny sdílení front.

#### ObjectProfile

Název objektu nebo generický profil, pro které chcete změnit autorizace.

#### GroupName

Název skupiny, ke které má být udělen přístup.

### Související informace

[Profily zabezpečení připojení pro inicializátor kanálu](#)

## 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 <a href="#">“Udělení oprávnění k získání zpráv z front” na stránce 369</a>
Kontext sady aplikací	Viz <a href="#">“Udělení oprávnění pro nastavení kontextu” na stránce 370</a>
Aplikace předává kontext	Viz <a href="#">“Udělení oprávnění pro předání kontextu” na stránce 371</a>
Aplikace ukládá zprávy do klastrované fronty.	Viz <a href="#">“Autorizace vkládání zpráv ve vzdálených frontách klastru” na stránce 405</a>
Aplikace vkládá zprávy do lokální fronty	Viz <a href="#">“Udělení oprávnění k vkládání zpráv do lokální fronty” na stránce 371</a>
Aplikace vkládá zprávy do modelové fronty	Viz <a href="#">“Udělení oprávnění k vkládání zpráv do modelové fronty” na stránce 372</a>
Aplikace vkládá zprávy do vzdálené fronty	Viz <a href="#">“Udělení oprávnění pro vkládání zpráv do vzdálené fronty klastru” na stránce 373</a>

### 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.

V systémech UNIX, Linux, Windows a IBM můžete také použít příkaz [SET AUTHREC](#).

**Poznámka:** V produktu IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC**.

## Procedura

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

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +get
```

- Pro IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*GET) MQMNAME(' QMgrName ')
```

- Pro z/OSzadejte následující příkazy:

```
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)  
PERMIT QMgrName.ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(UPDATE)
```

Názvy proměnných mají následující význam:

### QMgrName

Název správce front. V systému z/OS může být tato hodnota také názvem skupiny sdílení front.

### ObjectProfile

Název objektu nebo generický profil, pro které chcete změnit autorizace.

## GroupName

Název skupiny, ke které má být udělen přístup.

### Udělení oprávnění pro nastavení kontextu

Udělte oprávnění pro nastavení kontextu na zprávu, která je vložena, pro každou skupinu uživatelů, kteří pro ni potřebují obchodní potřeby.

## Informace o této úloze

Chcete-li udělit oprávnění pro nastavení kontextu v některých frontách, použijte příslušné příkazy pro daný operační systém.

V systémech UNIX, Linux, Windows a IBM můžete také použít příkaz `SET AUTHREC`.

**Poznámka:** V produktu IBM MQ Appliance můžete použít pouze příkaz `SET AUTHREC`.

## 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
```

**Poznámka:** Chcete-li použít oprávnění `setid` nebo `setall`, autorizace musí být udělena jak pro příslušný objekt fronty, tak i pro objekt správce front.

- Pro IBM izadejte jeden z následujících příkazů:

- Chcete-li nastavit pouze kontext identity:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*SETID) MQMNAME(' QMgrName ')
```

- Chcete-li nastavit celý kontext:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*SETALL) MQMNAME(' QMgrName ')
```

- Pro z/OSzadejte jednu z následujících sad příkazů:

- Chcete-li nastavit pouze kontext identity:

```
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)  
PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
```

- Chcete-li nastavit celý kontext:

```
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)  
PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(CONTROL)
```

Názvy proměnných mají následující význam:

### QMGrName

Název správce front. V systému z/OS může být tato hodnota také názvem skupiny sdílení front.

### ObjectProfile

Název objektu nebo generický profil, pro které chcete změnit autorizace.

## GroupName

Název skupiny, ke které má být udělen přístup.

### Udělení oprávnění pro předání kontextu

Udělte oprávnění pro předávání kontextu z načtené zprávy do každé skupiny uživatelů, kteří pro ni mají obchodní potřebu.

## Informace o této úloze

Chcete-li udělit oprávnění pro předávání kontextu v některých frontách, použijte příslušné příkazy pro daný operační systém.

V systémech UNIX, Linux, Windows a IBM můžete také použít příkaz [SET AUTHREC](#) .

**Poznámka:** V produktu IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

## 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 ')
```

- Chcete-li předat kontext identity nebo celý kontext, zadejte pro příkaz z/OSnásledující příkazy:

```
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)  
PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
```

Názvy proměnných mají následující význam:

### QMgrName

Název správce front. V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.

### ObjectProfile

Název objektu nebo generický profil, pro které chcete změnit autorizace.

### GroupName

Název skupiny, ke které má být udělen přístup.

### Udělení oprávnění k vkládání zpráv do lokální fronty

Udělte oprávnění pro vkládání zpráv do lokální fronty nebo sady front do každé skupiny uživatelů, kteří pro ni potřebují obchodní potřeby.



## Informace o této úloze

Chcete-li udělit oprávnění pro vkládání zpráv do některých lokálních front, použijte příslušné příkazy pro daný operační systém.

V systémech UNIX, Linux, Windows a IBM můžete také použít příkaz [SET AUTHREC](#) .

**Poznámka:** V produktu IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

## Procedura

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

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +put
```

- Pro IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*PUT) MQMNAME(' QMgrName ')
```

- Pro z/OSzadejte následující příkazy:

```
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)  
PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
```

Názvy proměnných mají následující význam:

### QMgrName

Název správce front. V systému z/OS může být tato hodnota také názvem skupiny sdílení front.

### ObjectProfile

Název objektu nebo generický profil, pro které chcete změnit autorizace.

### GroupName

Název skupiny, ke které má být udělen přístup.

*Udělení oprávnění k vkládání zpráv do modelové fronty*

Udělte oprávnění pro vkládání zpráv do modelové fronty nebo sady modelových front pro každou skupinu uživatelů, kteří pro ni potřebují obchodní potřeby.

## Informace o této úloze

Modelové fronty se používají k vytváření dynamických front. Musíte proto udělit oprávnění pro model i pro dynamické fronty. Chcete-li tyto oprávnění udělit, použijte příslušné příkazy pro váš operační systém.

V systémech UNIX, Linux, Windows a IBM můžete také použít příkaz [SET AUTHREC](#) .

**Poznámka:** V produktu IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

## 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 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/OS může být tato hodnota také názvem skupiny sdílení front.

#### **Název ModelQueue**

Název modelové fronty, na které jsou založeny dynamické fronty.

#### **ObjectProfile**

Název dynamické fronty nebo generický profil, pro které se mají změnit autorizace.

#### **GroupName**

Název skupiny, ke které má být udělen přístup.

### *Udělení oprávnění pro vkládání zpráv do vzdálené fronty klastru*

Udělte oprávnění pro vkládání zpráv do vzdálené fronty klastru nebo do fronty, do každé skupiny uživatelů, kteří pro ni potřebují obchodní potřeby.

## **Informace o této úloze**

Chcete-li vložit zprávu do fronty vzdáleného klastru, můžete ji buď umístit na lokální definici vzdálené fronty, nebo zcela kvalifikovanou vzdálenou frontu. Používáte-li lokální definici vzdálené fronty, potřebujete oprávnění k umístění lokálního objektu: viz [“Udělení oprávnění k vkládání zpráv do lokální fronty”](#) na stránce 371. 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.

V systémech UNIX, Linux, Windows a IBM můžete také použít příkaz [SET AUTHREC](#).

**Poznámka:** V produktu IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC**.

## **Procedura**

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

```
setmqaut -m QMgrName -t rqmname -n
ObjectProfile -g GroupName +put
```

Všimněte si, že můžete použít objekt `rqmname` pouze pro vzdálené fronty klastru.

- Pro IBM izadejte tento příkaz:

```
GRTMQMAUT OBJTYPE(*RMTMQMNAME) OBJ('
ObjectProfile') USER(GroupName) AUT(*PUT) MQMNAME('
QMgrName')
```

Všimněte si, že můžete použít objekt `RMTMQMNAME` pouze pro vzdálené fronty klastru.

- Pro z/OS zadejte následující příkazy:

```
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.QUEUE.ObjectProfile CLASS(MQQUEUE)
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/OS může být tato hodnota také názvem skupiny sdílení front.

**ObjectProfile**

Název vzdáleného správce front nebo generický profil, pro které chcete změnit autorizace.

**GroupName**

Název skupiny, ke které má být udělen přístup.

### Řízení přístupu uživatelů k tématům

Je třeba řídit přístup aplikací k tématům. Použijte toto téma k určení, jaké akce se mají provést.

Pro každý pravdivý příkaz v prvním sloupci proveďte akci uvedenou ve druhém sloupci.

Tabulka 69. Řízení přístupu uživatelů k tématům	
Příkaz	Akce
Aplikace publikuje zprávy do tématu	Viz <a href="#">“Udělení oprávnění pro publikování zpráv do tématu” na stránce 374</a>
Aplikace se přihlásí k odběru tématu.	Viz <a href="#">“Udělení oprávnění k odběru témat” na stránce 375</a>

#### 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.

V systémech UNIX, Linux, Windows a IBM můžete také použít příkaz [SET AUTHREC](#).

**Poznámka:** V produktu IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC**.

### Procedura

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

```
setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName +pub
```

- Pro IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*TOPIC) USER(GroupName) AUT(*PUB) MQMNAME(' QMgrName ')
```

- Pro z/OSzadejte následující příkazy:

```
RDEFINE MQTOPIC QMgrName.ObjectProfile UACC(NONE)  
PERMIT QMgrName.ObjectProfile CLASS(MQTOPIC) ID(GroupName) ACCESS(UPDATE)
```

Názvy proměnných mají následující význam:

**QMgrName**

Název správce front. V systému z/OS může být tato hodnota také názvem skupiny sdílení front.

**ObjectProfile**

Název objektu nebo generický profil, pro které chcete změnit autorizace.

### GroupName

Název skupiny, ke které má být udělen přístup.

#### Udělení oprávnění k odběru témat

Udělte oprávnění k odběru tématu nebo sady témat pro každou skupinu uživatelů, kteří pro ni mají obchodní potřebu.

### Informace o této úloze

Chcete-li udělit oprávnění přihlásit se k odběru některých témat, použijte příslušné příkazy pro váš operační systém.

V systémech UNIX, Linux, Windows a IBM můžete také použít příkaz [SET AUTHREC](#) .

**Poznámka:** V produktu IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

### Procedura

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

```
setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName +sub
```

- Pro IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*TOPIC) USER(GroupName) AUT(*SUB) MQMNAME(' QMgrName ')
```

- Pro z/OSzadejte následující příkazy:

```
RDEFINE MQTOPIC QMgrName.SUBSCRIBE.ObjectProfile UACC(NONE)  
PERMIT QMgrName.SUBSCRIBE.ObjectProfile CLASS(MQTOPIC) ID(GroupName) ACCESS(UPDATE)
```

Názvy proměnných mají následující význam:

#### QMgrName

Název správce front. V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.

#### ObjectProfile

Název objektu nebo generický profil, pro které chcete změnit autorizace.

#### GroupName

Název skupiny, ke které má být udělen přístup.

### Udělení oprávnění k dotazům na správce front

Udělte oprávnění k dotazům na správce front, do každé skupiny uživatelů, kteří pro ni potřebují obchodní potřeby.

### Informace o této úloze

Chcete-li udělit oprávnění k dotazům na správce front, použijte příslušné příkazy pro váš operační systém.

V systémech UNIX, Linux, Windows a IBM můžete také použít příkaz [SET AUTHREC](#) .

**Poznámka:** V produktu IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

### Procedura

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

```
setmqaut -m QMgrName -n ObjectProfile -t qmgr -g GroupName +inq
```

- Pro IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*MQM) USER(GroupName) AUT(*INQ) MQMNAME(' QMgrName')
```

- Pro z/OSzadejte následující příkazy:

```
RDEFINE MQCMD5 QMgrName.ObjectProfile UACC(NONE)  
PERMIT QMgrName.ObjectProfile CLASS(MQCMD5) ID(GroupName) ACCESS(READ)
```

Tyto příkazy udělují přístup k uvedenému správci front. Chcete-li uživateli povolit použití příkazu MQINQ, zadejte následující příkazy:

```
RDEFINE MQCMD5 QMgrName.MQINQ.QMGR UACC(NONE)  
PERMIT QMgrName.MQINQ.QMGR CLASS(MQCMD5) ID(GroupName) ACCESS(READ)
```

Názvy proměnných mají následující význam:

#### **QMgrName**

Název správce front. V systému z/OS může být tato hodnota také názvem skupiny sdílení front.

#### **ObjectProfile**

Název objektu nebo generický profil, pro které chcete změnit autorizace.

#### **GroupName**

Název skupiny, ke které má být udělen přístup.

### **Udělení oprávnění pro přístup k procesům**

Udělte oprávnění pro přístup k procesu nebo sadě procesů, pro každou skupinu uživatelů, kteří pro ni potřebují obchodní potřeby.

### **Informace o této úloze**

Chcete-li udělit oprávnění pro přístup k některým procesům, použijte příslušné příkazy pro váš operační systém.

V systémech UNIX, Linux, Windows a IBM můžete také použít příkaz [SET AUTHREC](#) .

**Poznámka:** V produktu IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC** .

### **Procedura**

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

```
setmqaut -m QMgrName -n ObjectProfile -t process -g GroupName +all
```

- Pro IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*PRC) USER(GroupName) AUT(*ALL) MQMNAME(' QMgrName')
```

- Pro z/OSzadejte následující příkazy:

```
RDEFINE MQPROC QMgrName.ObjectProfile UACC(NONE)  
PERMIT QMgrName.ObjectProfile CLASS(MQPROC) ID(GroupName) ACCESS(READ)
```

Názvy proměnných mají následující význam:

#### **QMgrName**

Název správce front. V systému z/OS může být tato hodnota také názvem skupiny sdílení front.

#### **ObjectProfile**

Název objektu nebo generický profil, pro které chcete změnit autorizace.

**GroupName**

Název skupiny, ke které má být udělen přístup.

**Udělení oprávnění pro přístup k seznamům názvů**

Udělte oprávnění pro přístup k seznamu názvů nebo sadě seznamů názvů, pro každou skupinu uživatelů, kteří pro ni potřebují obchodní položku.

**Informace o této úloze**

Chcete-li udělit oprávnění pro přístup k některým seznamům názvů, použijte příslušné příkazy pro váš operační systém.

V systémech UNIX, Linux, Windows a IBM můžete také použít příkaz `SET AUTHREC`.

**Poznámka:** V produktu IBM MQ Appliance můžete použít pouze příkaz **SET AUTHREC**.

**Procedura**

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

```
setmqaut -m QMgrName -n
ObjectProfile -t namelist -g GroupName
+all
```

- Pro IBM izadejte tento příkaz:

```
GRTMQMAUT OBJ('ObjectProfile
') OBJTYPE(*NMLIST) USER(GroupName) AUT(*ALL) MQMNAME('
QMgrName')
```

- Pro z/OSzadejte následující příkazy:

```
RDEFINE MQNLIST
QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile
CLASS(MQNLIST) ID(GroupName) ACCESS(READ)
```

Názvy proměnných mají následující význam:

**QMgrName**

Název správce front. V systému z/OSmůže být tato hodnota také názvem skupiny sdílení front.

**ObjectProfile**

Název objektu nebo generický profil, pro které chcete změnit autorizace.

**GroupName**

Název skupiny, ke které má být udělen přístup.

**Oprávnění k administraci produktu IBM MQ v systémech SYSTÉM UNIX, Linux a Okna**

Administrátoři produktu IBM MQ mohou používat všechny příkazy produktu IBM MQ a udělovat oprávnění ostatním uživatelům. Když administrátoři vydají příkazy vzdáleným správcům front, musí mít požadované oprávnění ve vzdáleném správci front. Další pokyny platí pro systémy Windows.

Administrátoři produktu IBM MQ mají oprávnění k používání všech příkazů produktu IBM MQ (včetně příkazů pro udělení oprávnění IBM MQ jiným uživatelům)

Chcete-li být administrátorem produktu IBM MQ, musíte být členem speciální skupiny s názvem skupiny `mqm`.

**Windows** Případně pouze v systému Windows můžete být členem skupiny Administrators na systémech Windows.

Skupina mqm se vytvoří automaticky při instalaci produktu IBM MQ ; přidejte další uživatele do skupiny a umožněte 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 ke správě produktu IBM MQ. Jeden z těchto řídicích příkazů je **setmqaut**, který se používá k udělení oprávnění jiným uživatelům, aby jim bylo umožněno přistupovat k prostředkům IBM MQ nebo řídit jejich řízení. Příkazy PCF pro správu záznamů oprávnění jsou 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 musí mít požadovaná oprávnění pro příkazy MQSC, které mají být zpracovány vzdáleným správcem front. Program IBM MQ Explorer vydává příkazy PCF pro provádění administrativních úloh. Administrátoři nepotřebují další oprávnění k používání Průzkumníka IBM MQ ke správě správce front v lokálním systému. Pokud se Průzkumník IBM MQ používá ke správě správce front v jiném systému, administrátoři musí mít požadovaná oprávnění pro příkazy PCF, které mají být zpracovány vzdáleným správcem front.



**Upozornění:** Z produktu IBM MQ 8.0 nemusíte být administrátorem, abyste mohli použít řídicí příkaz **runmqsc**, který vydává příkazy skriptu IBM MQ Script (MQSC).

Je-li produkt **runmqsc** použit v nepřímém režimu k odeslání příkazů MQSC do vzdáleného správce front, je každý příkaz MQSC zapouzdřen v rámci příkazu Escape PCF.

Další informace o kontrolách oprávnění, jsou-li zpracovány příkazy PCF a MQSC, najdete v následujících tématech:

- Pro příkazy PCF, které pracují se správci front, frontami, procesy, seznamy názvů a objekty ověřovacích informací, viz [Oprávnění pro práci s objekty IBM MQ](#). Informace o ekvivalentních příkazech MQSC zapouzdřených v příkazech Escape PCF najdete v této sekci.
- Pro příkazy PCF, které pracují s kanály, inicializátory kanálu, listenery a klastry, naleznete informace v tématu [Zabezpečení kanálů](#).
- Pro příkazy PCF, které pracují se záznamy oprávnění, viz [Kontrola oprávnění pro příkazy PCF](#)
-  U příkazů MQSC, které jsou zpracovány příkazovým serverem v systému IBM MQ for z/OS, naleznete informace v tématu [Zabezpečení příkazů a zabezpečení prostředků příkazů v systému z/OS](#).

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

Na platformách SYSTÉM UNIX a Linux je rovněž vytvořeno speciální ID uživatele mqm, které je možné použít pouze pro produkt. Nesmí být nikdy k dispozici pro neprivilégované uživatele. Všechny objekty produktu IBM 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 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 381.

Windows verzí s funkcí UAC (User Account Control) omezuje akce, které mohou uživatelé provádět na určitých zařízeních operačního systému, i když jsou členy skupiny Administrators. Je-li vaše ID uživatele ve skupině administrátorů, ale ne skupině mqm, musíte použít zvýšený příkazový řádek k vydání příkazů administrátora produktu IBM MQ , jako je například **crtmqm**, v opačném případě je vygenerována chyba AMQ7077: Nemáte oprávnění k provedení požadované operace . Chcete-li otevřít příkazový řádek se zvýšeným oprávněním, klepněte pravým tlačítkem myši na položku nabídky Start nebo na ikonu na příkazový řádek a vyberte volbu **Spustit jako administrátor**.

Chcete-li provést následující akce, nemusíte být členem skupiny mqm:



- Vydejte příkazy z aplikačního programu, který vydává příkazy PCF, nebo příkazy MQSC v příkazu Escape PCF, pokud příkazy manipulují inicializátory kanálu. (Tyto příkazy jsou popsány v části [“Zabezpečení definic inicializátoru kanálu”](#) na stránce 97 ).
- Vydejte volání MQI z aplikačního programu (pokud nechcete použít vazby rychlé cesty na volání MQCONN).
- Příkaz `ctrlmqcvx` se používá k vytvoření fragmentu kódu, který provádí převod dat na strukturách datových typů.
- Chcete-li zobrazit správce front, použijte příkaz `dspmq` .
- Příkaz `dspmqttrc` se používá k zobrazení formátovaného výstupu trasování IBM MQ .

Omezení 12 znaků se týká jak skupin, tak ID uživatelů.

Platformy SYSTÉM UNIX a Linux obecně omezují délku ID uživatele na 12 znaků. Produkt AIX verze 5.3 tento limit zvýšil, ale produkt IBM MQ i nadále dodržuje omezení 12 znaků na všech platformách SYSTÉM UNIX a Linux . Použijete-li ID uživatele větší než 12 znaků, nahradí jej produkt IBM MQ hodnotou UNKNOWN . Nedefinujte ID uživatele s hodnotou UNKNOWN .

## Správa skupiny mqm

Uživatelům v skupině mqm jsou udělena úplná administrativní oprávnění k produktu IBM MQ. Z tohoto důvodu byste neměli zapisovat aplikace a běžné uživatele do skupiny mqm. Skupina mqm by měla obsahovat pouze účty administrátorů produktu IBM MQ .

Tyto úlohy jsou popsány v následujících tématech:

- [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 vaší domény nastavit speciální účet, který má produkt IBM MQ používat. Další informace viz [Konfigurace IBM MQ s Prepare IBM MQ Wizard](#) a [Vytvoření a nastavení Windows účtů domény pro IBM MQ](#).

## Oprávnění pro práci s objekty IBM MQ v systémech UNIX, Linux a Windows

Všechny objekty jsou chráněny produktem IBM MQ a činitelé musí mít odpovídající oprávnění pro přístup k nim. Různí činitelé potřebují různá přístupová práva k různým objektům.

Správci front, fronty, definice procesů, seznamy názvů, kanály, kanály připojení klienta, moduly listener, služby a objekty ověřovacích informací jsou všechny přístupné z aplikací, které používají volání MQI nebo příkazy PCF. Tyto prostředky jsou všechny chráněny produktem IBM MQ a aplikace musí mít oprávnění k přístupu k nim. Entita, která vydává požadavek, může být uživatel, aplikační program, který vydává volání MQI, nebo administrativní program, který vydává příkaz PCF. Identifikátor žadatele je označován jako *činitel*.

Různým skupinám činitelů lze udělit různé typy přístupových oprávnění ke stejnému objektu. Například u určité fronty může být jedna skupina povolena k 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 systému Windows).

### **Související pojmy**

“Oprávnění k administraci produktu IBM MQ v systémech SYSTÉM UNIX, Linux a Okna” na stránce 377  
Administrátoři produktu IBM MQ mohou používat všechny příkazy produktu IBM MQ a udělovat oprávnění ostatním uživatelům. Když administrátoři vydají příkazy vzdáleným správcům front, musí mít požadované oprávnění ve vzdáleném správci front. Další pokyny platí pro systémy Windows.

## **Když jsou provedeny kontroly zabezpečení systémů UNIX, Linux a Windows**

Kontroly zabezpečení jsou obvykle prováděny při připojování ke správci front, při otevírání nebo zavírání objektů a při vkládání nebo načítání zpráv.

Kontroly zabezpečení provedené pro typickou aplikaci jsou následující:

### **Připojování ke správci front (volání MQCONN nebo MQCONNX)**

Toto je poprvé, kdy je aplikace asociována s konkrétním správcem front. Správce front dotazuje operační prostředí ke zjištění ID uživatele přidruženého k aplikaci. Produkt IBM MQ potom ověřuje, zda je ID uživatele autorizováno pro připojení ke správci front, a zachová ID uživatele pro budoucí kontroly.

Uživatelé se nemusí přihlašovat k produktu IBM MQ; produkt IBM MQ předpokládá, že uživatelé se přihlásili k základnímu operačnímu systému a byli ověřeni tímto způsobem.

### **Otevření objektu (volání MQOPEN nebo MQPUT1)**

K objektům produktu IBM MQ se přistupuje otevřením objektu a zadáním jeho příkazů. Všechny kontroly prostředků se provádějí při otevření objektu, spíše než při jejich skutečném přístupu. To znamená, že požadavek **MQOPEN** musí uvádět požadovaný typ přístupu (například to, zda uživatel chce pouze procházet objekt nebo provést aktualizaci jako vkládání zpráv do fronty).

Produkt IBM MQ zkontroluje prostředek, který je uveden v požadavku **MQOPEN**. Pro alias nebo objekt vzdálené fronty je použita autorizace sama o sobě pro objekt, nikoli frontu, na kterou je rozlišen alias nebo vzdálená fronta. To znamená, že uživatel nepotřebuje oprávnění pro přístup k němu. Omezte oprávnění k vytváření front pro privilegované uživatele. Pokud tomu tak není, uživatelé mohou obejít normální řízení přístupu pouhým vytvořením aliasu. Je-li vzdálená fronta odkazována explicitně spolu s názvy fronty i správce front, je zkontrolována přenosová fronta přidružená ke vzdálenému správci front.

Oprávnění k dynamické frontě je založeno na tom, které z modelové fronty je odvozeno, ale nemusí být nutně stejné. Tento popis je popsán v poznámce [“1”](#) na stránce 122.

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)**

Nepovedou se žádné kontroly řízení přístupu.

### **Zavření objektu (MQCLOSE)**

Nejsou provedeny žádné kontroly řízení přístupu, pokud **MQCLOSE** nezpůsobuje odstranění dynamické fronty. V takovém případě je zde kontrola, že ID uživatele je oprávněno k odstranění fronty.

### **Přihlášení k odběru tématu (MQSUB)**

Když se aplikace přihlašuje k odběru tématu, určuje typ operace, kterou je třeba provést. Jedná se o vytvoření nového odběru, změnu existujícího odběru nebo obnovení existujícího odběru, aniž by došlo k jeho změně. Pro každý typ operace správce front ověří, zda má ID uživatele přidružené k aplikaci oprávnění k provedení operace.

Když se aplikace přihlásí k odběru tématu, provede se kontrola oprávnění k objektům tématu, které se nacházejí ve stromu témat ve stromu témat, v němž je aplikace odebírána, nebo nad ním. Kontroly oprávnění mohou zahrnovat kontroly více než jednoho objektu tématu.

ID uživatele, které správce front používá pro kontrolu oprávnění, je ID uživatele získané z operačního systému, když se aplikace připojuje ke správci front.

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

## Jak řízení přístupu je implementováno produktem IBM MQ v systémech UNIX, Linux a Windows

Produkt IBM MQ používá služby zabezpečení poskytované podkladovým operačním systémem pomocí správce oprávnění k objektu. IBM MQ poskytuje příkazy pro vytváření a údržbu seznamů přístupových práv.

Součástí produktu IBM MQ je rozhraní řízení přístupu, které se nazývá rozhraní služeb autorizace. Produkt IBM MQ poskytuje implementaci správce řízení přístupu (vyhovujícího rozhraní autorizační služby) označovaným jako *správce oprávnění k objektu (OAM)*. Toto je automaticky nainstalováno a povoleno pro každého správce front, kterého jste vytvořili, pokud neurčíte jinak (jak je popsáno v [“Prevence kontrol přístupu k zabezpečení v systémech Windows, SYSTÉM UNIX a Linux”](#) na stránce 342). OAM může být nahrazen libovolným uživatelem nebo dodavatelem zapsanou komponentou, která je v souladu s rozhraním autorizační služby.

OAM využívá funkce zabezpečení základního operačního systému s použitím ID uživatelů a skupin operačního systému. Uživatelé mohou přistupovat k objektům produktu IBM MQ pouze v případě, že mají správné oprávnění. [“Řízení přístupu k objektům pomocí OAM v systémech UNIX, Linux a Windows”](#) na stránce 334 popisuje, jak tento úřad udělit a odvolat.

OAM udržuje seznam přístupových práv (ACL) pro každý prostředek, který řídí. Data autorizace jsou uložena v lokální frontě s názvem SYSTEM.AUTH.DATA.QUEUE. Přístup k této frontě je omezen na uživatele ve skupině mqm a dále na Windowsuživatelům ve skupině administrátorů a uživatelé se přihlásili s ID SYSTEM. Uživatelský přístup ke frontě nelze změnit.

IBM MQ poskytuje příkazy pro vytváření a údržbu seznamů přístupových práv. Další informace o těchto příkazech najdete v tématu [“Řízení přístupu k objektům pomocí OAM v systémech UNIX, Linux a Windows”](#) na stránce 334.

Produkt IBM MQ předává požadavek OAM požadavek obsahující činitel, název prostředku a typ přístupu. OAM uděluje nebo odmítá přístup na základě seznamu ACL, který spravuje. IBM MQ dodržuje rozhodnutí OAM; pokud OAM nemůže učinit rozhodnutí, IBM MQ neumožňuje přístup.

## Identifikace ID uživatele v systémech Windows, SYSTÉM UNIX a Linux

Správce oprávnění k objektu identifikuje činitele, který žádá o přístup k prostředku. ID uživatele použité jako činitel se liší v závislosti na kontextu.

Správce oprávnění k objektu (OAM) musí být schopen identifikovat, kdo žádá o přístup k určitému prostředku. IBM MQ používá termín *činitel* k odkazování na tento identifikátor. Činitel je vytvořen při prvním připojení aplikace ke správci front; je určen správcem front z ID uživatele přidruženého k připojované aplikaci. (Pokud aplikace odesílá volání XA bez připojení ke správci front, bude ID uživatele přidružené k aplikaci, které vydává volání xa\_open, použito pro kontrolu oprávnění správce front.)

V systémech SYSTÉM UNIX a Linux autorizační rutiny kontrolují buď skutečné ID uživatele (logged-in), nebo efektivní ID uživatele přidružené k aplikaci. Zaškrtnuté ID uživatele může záviset na typu vazby, aby se zobrazily podrobnosti v části [Instalovatelné služby](#).

IBM MQ šíří ID uživatele přijaté ze systému v záhlaví zprávy (struktura MQMD) pro každou zprávu jako identifikaci uživatele. Tento identifikátor je součástí informací o kontextu zprávy a je popsán v části [“Autorita kontextu v systémech UNIX, Linux a Windows”](#) na stránce 384. Aplikace nemohou tyto informace měnit, pokud nemají autorizaci ke změně informací o kontextu.

### Činitelé a skupiny

Řídící služby mohou náležet do skupin. Tím, že udělíte přístup k prostředkům spíše skupinám než jednotlivcům, můžete snížit požadované množství administrace. Seznamy přístupových práv (ACL) jsou založeny na skupinách i ID uživatelů.

Můžete například definovat skupinu skládající se z uživatelů, kteří chtějí spustit určitou aplikaci. Ostatní uživatelé mohou mít přístup ke všem prostředkům, které vyžadují, přidáním jejich ID uživatele do příslušné skupiny.

Tento proces definování a správy skupin je popsán pro konkrétní platformy:

- [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 jeho PCF).

### Systémy SYSTÉM UNIX a Linux

V produktu Verze 8.0 jsou seznamy přístupových práv (ACL) založeny na identifikátorech uživatelů a skupinách a lze je použít buď pro autorizaci nastavením atributu **SecurityPolicy** na příslušnou hodnotu, jak je popsáno v [Instalovatelných službách](#), a [Konfigurace stanz autorizační služby](#) v systému UNIX a Linux.

V produktu Verze 8.0 můžete pro autorizaci použít *model založený na uživateli* a můžete použít jak uživatele, tak skupiny. Když však uvedete uživatele v příkazu `setmqaut`, nová oprávnění se vztahují pouze na tohoto uživatele a ne na skupiny, do kterých tento uživatel patří. Další informace naleznete v tématu [Oprávnění založená na uživateli v systémech Unix a Linux](#).

Použijete-li pro autorizaci *model založený na skupině*, bude do seznamu přístupových práv zahrnuta primární skupina, do níž patří toto ID uživatele. Individuální ID uživatele není zahrnuto a oprávnění je uděleno všem členům této skupiny. Vzhledem k tomu si buďte vědomi toho, že můžete nechtěně změnit oprávnění činitele změnou oprávnění jiného činitele ve stejné skupině.

Všichni uživatelé jsou přiřazeni k výchozí skupině uživatelů nobody a ve výchozím nastavení nejsou této skupině udělena žádná autorizace. Autorizaci ve skupině nobody můžete změnit, chcete-li uživatelům bez specifických autorizací udělit přístup k prostředkům produktu IBM MQ.

Nedefinujte ID uživatele s hodnotou UNKNOWN. Hodnota UNKNOWN se používá, když je ID uživatele příliš dlouhé, takže libovolné ID uživatele budou používat přístupová oprávnění UNKNOWN.

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 Systémy SYSTÉM UNIX. V různých doménách můžete mít různé uživatele se stejným ID uživatele. IBM MQ povoluje, aby ID uživatelů byla kvalifikována jménem domény, takže těmto uživatelům mohou být poskytnuty různé úrovně přístupu.

Název skupiny může volitelně zahrnovat název domény, uvedený v následujících formátech:

```
GroupName@domain domain_name\group_name
```

Globální skupiny kontroluje OAM pouze ve dvou případech:

1. Oddíl zabezpečení správce front obsahuje nastavení: `GroupModel=GlobalGroups`. Viz [Zabezpečení](#).
2. Správce front používá alternativní skupinu přístupů zabezpečení. Viz [crtmqm](#).

ID uživatele mohou obsahovat až 20 znaků, názvy domén až 15 znaků a názvy skupin až 64 znaků.

OAM nejprve zkontroluje lokální databázi zabezpečení, pak databázi primární domény a nakonec databázi všech důvěryhodných domén. První zjištěné ID uživatele používá OAM pro kontrolu. Každé z těchto ID uživatelů může mít odlišná členství ve skupině na konkrétním počítači.

Některé řídicí příkazy (například **crtmqm**) mění oprávnění k objektům IBM MQ pomocí správce oprávnění objektu (OAM). OAM prohledá databáze zabezpečení v pořadí uvedeném v předchozím odstavci, aby určila oprávnění pro konkrétní ID uživatele. V důsledku toho může oprávnění určené OAM přepsat skutečnost, že ID uživatele je členem lokální skupiny mqm. Pokud například zadáte příkaz **crtmqm** z ID uživatele ověřeného pomocí řadiče domény, který má členství v lokální skupině mqm prostřednictvím globální skupiny, příkaz selže, pokud má systém lokálního uživatele se stejným jménem, který není v lokální skupině mqm.

Další informace o nastavení atributu **SecurityPolicy** v systému Windows naleznete v tématech [Instalovatelné služby](#) a [Konfigurace oddílů autorizační služby v systému Windows](#).

### **Identifikátory zabezpečení produktu Windows (SID)**

Produkt IBM MQ v systému Windows používá SID, kde je k dispozici. Pokud není Windows SID dodán s autorizačním požadavkem, produkt IBM MQ identifikuje uživatele na základě samotného jména uživatele, ale to může mít za následek udělení chybného oprávnění.

V systému Windows se identifikátor zabezpečení (SID) používá k doplnění ID uživatele. Identifikátor SID obsahuje informace identifikující úplné podrobnosti o účtu uživatele na databázi správce účtů zabezpečení produktu Windows (SAM), kde je uživatel definován. Je-li vytvořena zpráva v systému IBM MQ for Windows, produkt IBM MQ ukládá identifikátor SID v deskriptoru zpráv. Když produkt IBM MQ na systému Windows provádí kontroly autorizace, použije identifikátor SID k získání dotazu na úplné informace z databáze SAM. (Databáze SAM, v níž je uživatel definován, musí být přístupná pro tento dotaz, aby byl úspěšný.)

By default, if a Windows SID is not supplied with an authorization request, IBM MQ identifies the user based on the user name alone. To provádět prohledávání databází zabezpečení v následujícím pořadí:

1. Lokální databáze zabezpečení
2. Databáze zabezpečení primární domény
3. Databáze zabezpečení důvěryhodných domén

Není-li jméno uživatele jedinečné, může být uděleno nesprávné oprávnění IBM MQ. Chcete-li tomuto problému předejít, zahrňte do každého požadavku na autorizaci identifikátor SID; identifikátor SID je použit produktem IBM MQ k vytvoření pověření uživatele.

Chcete-li zadat, že všechny požadavky na autorizaci musí obsahovat SID, použijte `regedit`. Nastavte `SecurityPolicy` na `NTSIDsRequired`.

### **Oprávnění alternativního uživatele v systémech UNIX, Linux a Windows**

Můžete uvést, že ID uživatele může použít oprávnění jiného uživatele při přístupu k objektu IBM MQ. Tento příkaz se nazývá *oprávnění alternativního uživatele* a můžete jej použít na libovolném objektu IBM MQ.

Oprávnění alternativního uživatele je nezbytné, pokud server přijímá požadavky od programu a chce se ujistit, že má program požadované oprávnění pro tento požadavek. Server může mít požadované oprávnění, ale musí vědět, zda má tento program oprávnění pro akce, které požadoval.

Předpokládejme například, že serverový program spuštěný pod ID uživatele PAYSERV načte zprávu požadavku z fronty, která byla vložena do fronty, pomocí ID uživatele USER1. Když serverový program získá zprávu požadavku, zpracuje požadavek a vrátí odpověď zpět do fronty pro odpověď, která je uvedena spolu se zprávou požadavku. Server může namísto použití vlastního ID uživatele (PAYSERV) autorizovat otevření fronty pro odpověď. Server může v tomto případě určit jiné ID uživatele, USER1. V tomto příkladu můžete použít alternativní oprávnění k řízení, zda má PAYSERV povoleno zadat USER1 jako alternativní ID uživatele při otevření fronty pro odpověď.

ID alternativního uživatele je určeno v poli **AlternateUserId** deskriptoru objektu.

## 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`, `AccountingToken` a `AppIdentityData` .

### Sekce Původ

Místo, odkud zpráva přišla, a kdy byla vložena do fronty. Skládá se z polí `PutAppType`, `PutAppName`, `PutDate`, `PutTime` a `AppOriginData` .

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 IBM MQ . Zejména počáteční hodnota jednoho z polí, `MCAUserIdentifier`, je určena hodnotou parametru `MCAUSER` v příkazu `DEFINE CHANNEL`, nebo ekvivalentní hodnotě `MCAUSER`, pokud je definice kanálu vytvořena jiným způsobem.

Struktura MQCD je předána výstupnímu programu kanálu, pokud je volána programem MCA. Je-li uživatelská procedura pro zabezpečení volána prostřednictvím programu MCA, může uživatelská procedura zabezpečení změnit hodnotu parametru `MCAUserIdentifier` nahradit jakoukoli hodnotu zadanou v definici kanálu.

U systémů IBM i, UNIX, Linux a Windows , pokud hodnota `MCAUserIdentifier` je prázdná, používá správce front hodnotu `MCAUserIdentifier` jako ID uživatele pro kontroly oprávnění, když se agent MCA pokusí o přístup k prostředkům správce front poté, co se připojí 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/OS může správce front použít hodnotu `MCAUserIdentifier` pro kontroly oprávnění, pokud tato hodnota není prázdná. For receiving MCAs and server connection MCAs, whether the queue manager uses the value of `MCAUserIdentifier` for authority checks depends on:

- Hodnota parametru `PUTAUT` v definici kanálu
- Profil produktu RACF použitý pro kontroly
- Úroveň přístupu ID uživatele adresního prostoru iniciátoru kanálu do profilu `RESLEVEL`

Pro posílání MCA to závisí na:

- Zda je odesílající agent MCA volajícím nebo respondentem



- Úroveň přístupu ID uživatele adresního prostoru iniciátoru kanálu do profilu RESLEVEL

ID uživatele, které se ukládá do úložiště uživatelské procedury zabezpečení v *MCAUserIdentifier*, lze získat různými způsoby. Některé příklady:

- Pokud na konci klienta kanálu MQI neexistuje žádná uživatelská procedura zabezpečení, ID uživatele přidružené k aplikačním aplikacím klienta produktu IBM MQ přechází z klienta MCA pro připojení klienta do kanálu MCA připojení k serveru, když aplikace klienta odešle volání MQCONN.Agent MCA pro připojení k serveru ukládá toto ID uživatele do pole *RemoteUserIdentifier* ve struktuře definice kanálu, MQCD. Je-li hodnota *MCAUserIdentifier* prázdná, v prostředí MCA se uloží stejné ID uživatele v *MCAUserIdentifier*. Pokud agent MCA neukládá ID uživatele v souboru *MCAUserIdentifier*, může uživatelská procedura zabezpečení provést tuto akci později nastavením *MCAUserIdentifier* na hodnotu *RemoteUserIdentifier*.

Pokud ID uživatele, které teče ze systému klienta, vstupuje do nové domény zabezpečení a není v systému serveru platné, může uživatelská procedura zabezpečení nahradit ID uživatele, která je platná, a uložit nahrazené ID uživatele v souboru *MCAUserIdentifier*.

- ID uživatele může být odesláno uživatelskou procedurou zabezpečení ochrany dat ve zprávě zabezpečení.

Na kanálu zpráv může uživatelská procedura zabezpečení odesílající agent MCA odeslat ID uživatele, pod kterým je odesílající agent MCA spuštěn. Uživatelská procedura zabezpečení volaná přijímajícím agentem MCA může poté uložit ID uživatele do souboru *MCAUserIdentifier*. Podobně na kanálu MQI může uživatelská procedura zabezpečení na straně klienta kanálu odeslat ID uživatele přidružené k aplikaci produktu IBM MQ MQI client. Uživatelská procedura zabezpečení na konci serveru kanálu pak může uložit ID uživatele do souboru *MCAUserIdentifier*. Stejně jako v předchozím příkladu, pokud ID uživatele není platné na cílovém systému, může uživatelská procedura zabezpečení nahradit ID uživatele platnou a uložit nahrazené ID uživatele v souboru *MCAUserIdentifier*.

Je-li jako součást identity a ověřovací služby přijat digitální certifikát, může uživatelská procedura pro zabezpečení mapovat rozlišující název v certifikátu na ID uživatele, které je platné na cílovém systému. Pak může uložit ID uživatele do *MCAUserIdentifier*.

- Je-li 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:** Aplikace uživatelské procedury zabezpečení vytvořené před vydáním produktu IBM MQ v7.1 mohou vyžadovat aktualizaci. Další informace najdete v tématu [Uživatelské programy zabezpečení kanálu](#).

## OVĚŘENÍ UŽIVATELE SPRÁVCE OPRAVNĚNÍ OBJEKTU IBM MQ

V případě IBM MQ MQI client připojení lze k úpravě nebo vytvoření struktury MQCSP použité v ověření uživatele správce oprávnění k objektu (OAM) použít uživatelské procedury zabezpečení. To je popsáno v tématu [Programy výstupního bodu kanálů pro kanály systému zpráv](#)

## Implementace řízení přístupu ve výstupních procedurách zprávy

Může být nutné použít uživatelskou proceduru pro nahrazení jednoho ID uživatele jiným.

Uvažte aplikaci klienta, která odešle zprávu do serverové aplikace. Serverová aplikace může extrahovat ID uživatele z pole *UserIdentifier* v deskriptoru zprávy a za předpokladu, že má alternativní oprávnění uživatele, požádat správce front o použití tohoto ID uživatele pro kontrolu oprávnění při přístupu k prostředkům produktu IBM MQ v zastoupení klienta.

Je-li parametr PUTAUT nastaven na CTX (nebo ALTMCA na systému z/OS) V definici kanálu se ID uživatele v poli *UserIdentifier* každé příchozí zprávy používá pro kontrolu oprávnění, když agent MCA otevře cílovou frontu.

Za určitých okolností se při generování zprávy o sestavě použije oprávnění ID uživatele v poli *UserIdentifier* zprávy způsobující tuto sestavu. Zejména sestavy potvrzení o doručení (COD) a sestavy o vypršení platnosti jsou vždy s tímto oprávněním zavedeny.

Vzhledem k těmto situacím může být nezbytné nahradit jedno ID uživatele pro jinou v poli *UserIdentifier*, protože zpráva vstoupí do nové domény zabezpečení. To lze provést ukončením 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 320.

## Implementace řízení přístupu ve výstupu rozhraní API a ukončení přeletu rozhraní API

Rozhraní API nebo uživatelská procedura překřížení rozhraní API může poskytnout řízení přístupu k doplnění položek poskytovaného produktem IBM MQ. Ukončení může poskytovat řízení přístupu na úrovni zpráv. Uživatelská procedura může zajistit, že aplikace bude umístěna do fronty nebo se dostane z fronty, pouze ty zprávy, které splňují určitá kritéria.

Zvažte následující příklady:

- Zpráva obsahuje informace o objednávce. Když se aplikace pokusí vložit zprávu do fronty, rozhraní API nebo výstupní bod rozhraní API může zkontrolovat, zda celková hodnota objednávky je menší než stanovená mezní hodnota.
- Zprávy dorazí do cílové fronty ze vzdálených správců front. Když se aplikace pokusí získat zprávu z fronty, rozhraní API nebo uživatelská procedura rozhraní API může zkontrolovat, zda je odesílatel zprávy autorizován k odeslání zprávy do fronty.

### V 8.0.0.2 Přehled autorizace LDAP

Přehled toho, jak použijete autorizaci LDAP k odebrání potřeby lokálního ID uživatele.

Příkazy, které obsluhují konfiguraci autorizace, jako např. `setmqaut` a `DISPLAY AUTHREC`, mohou nyní zpracovávat rozlišující názvy. Dříve byli uživatelé ověřováni porovnáním jejich pověření s maximálním počtem dostupných znaků, které existují pro uživatele a skupiny v lokálním operačním systému.



**Upozornění:** Pokud jste spustili příkaz `DEFINE AUTHINFO`, musíte restartovat správce front. Pokud nerestartujete správce front, příkaz `setmqaut` nevrátí správný výsledek.

Pokud uživatel zadá ID uživatele, spíše než rozlišující název, bude ID uživatele zpracováno. Je-li například na kanálu s parametrem `PUTAUT (CTX)` příchozí zpráva, jsou znaky v ID uživatele mapovány na rozlišující název služby LDAP a jsou provedeny příslušné kontroly autorizace.

Další příkazy jako `DISPLAY CONN` budou nadále pracovat se skutečnou hodnotou pro ID uživatele i přesto, že ID uživatele nemusí ve skutečnosti existovat v lokálním operačním systému.

Je-li autorizace LDAP na místě, správce front vždy použije uživatelský model zabezpečení na platformách UNIX bez ohledu na atribut **SecurityPolicy** v souboru `qm.ini`. Takže nastavení oprávnění pro jednotlivého uživatele ovlivní pouze tohoto uživatele, a ne kohokoli jiného, kdo patří do některé z těchto skupin uživatelů.

Stejně jako u modelu OS má uživatel stále kombinované oprávnění, které bylo přiřazeno jak k jednotlivému, tak ke všem skupinám (pokud existují), ke kterému uživatel patří.

Předpokládejme například, že v úložišti LDAP byly definovány následující záznamy.

- Ve třídě **inetOrgPerson** :

```
dn="cn=JohnDoe, ou=users, o=yourcompany, c=yourcountry"
email=JohnDoe1@yourcompany.com [longer than 12 characters]
shortu=jodoe
Phone=1234567
```

- Ve třídě **groupOfNames** :

```
dn="cn=Application Group A, ou=groups, o=yourcompany, c=yourcountry"
longname=ApplicationGroupA [longer than 12 characters]
members="cn=JaneDoe, ou=users, o=yourcompany, c=yourcountry",
"cn=JohnDoe, ou=users, o=yourcompany, c=yourcountry"
```

Pro účely ověření musí být správce front používající tento server LDAP definován tak, aby jeho hodnota CONNAUTH ukazovala na objekt AUTHINFO typu IDPWLDAP a jehož relevantní atributy pro rozeznání názvů jsou pravděpodobně nastaveny takto:

```
USRFIELD(email) SHORTUSR(shortu)
BASEDNU(ou=users,o=yourcompany,c=yourcountry) CLASSUSR(inetOrgPerson)
```

Vzhledem k této konfiguraci pro ověření může aplikace vyplnit pole CSPUserID, které se používá v rámci volání MQCNO, s některou z následujících sad hodnot:

```
" cn=JohnDoe ", " JohnDoe1@yourcompany.com ", " email=JohnDoe1@yourcompany.com "
```

, nebo

```
" cn=JohnDoe, ou=users, o=ibm, c=uk ", " shortu=jodoe "
```

V obou případech může systém použít zadané hodnoty k ověření kontextu operačního systému " jodoe".

## Povolení autorizace LDAP na podporovaných platformách

Autorizace protokolu LDAP je k dispozici na následujících platformách:

- UNIX
- IBM i

### Důležité:

Chcete-li povolit konfiguraci nového modelu autorizace, je třeba nejprve změnit úroveň příkazů správce front tak, aby byla vyšší než úroveň obecné dostupnosti IBM MQ verze 8.0.0.0 800.

Musíš to udělat výslovně. Změna se neprovádí automaticky pomocí instalace opravné sady. Příklad:

```
stimqm -e CMDLEVEL=802 <qmname>
stimqm <qmname>
```

Pokud jste nastavili **CMDLEVEL** na 802, můžete odvolat opravu FixPack za předpokladu, že jste tuto novou funkci nepoužili.

Úroveň příkazů správce front řídí, zda lze provést změny konfigurace, které mají vliv na autorizaci, či nikoli. Po této změně můžete vidět a upravit nové atributy v objektu AUTHINFO.

Pokusíte-li se o přístup k novým atributům AUTHINFO z upgradované úrovně kódu, aniž byste také aktualizovali úroveň příkazů, obdržíte chybovou zprávu o potřebě změnit úroveň příkazů.

Všimněte si, že úroveň příkazu nemá žádný přímý vztah k verzi, vydání, úpravě, úrovni opravné sady.



## Nastavení oprávnění

Jak použijete krátký název nebo **USRFIELD** k nastavení autorizací.

Přístup k práci s více formáty, jak je popsáno v “Přehled autorizace LDAP” na stránce 386, pokračuje do autorizačních příkazů s dalším rozšířením, které lze použít v nezdobeném módu buď pro shortname , nebo pro USRFIELD.

Znakový řetězec uvádí konkrétní atribut v záznamu LDAP, když pojmenováváte uživatele (činitele) pro autorizaci.

**Důležité:** Znakový řetězec nesmí obsahovat znak = , protože tento znak nemůže být použit v ID uživatele operačního systému.

Předáte-li OAM základní jméno pro autorizaci, která je potencionálně shortname, musí se znakový řetězec vejít do 12 znaků. Algoritmus mapování se nejprve pokusí o jeho vyřešení na DN pomocí atributu SHORTUSR ve svém dotazu LDAP.

Pokud to selže s chybou UNKNOWN\_ENTITY nebo pokud daný řetězec nemůže být shortname, je proveden další pokus pomocí atributu USRFIELD k vytvoření dotazu LDAP.



**Upozornění:** Pokud jste spustili příkaz DEFINE AUTHINFO, musíte restartovat správce front. Pokud nerestartujete správce front, příkaz `setmqaut` nevrátí správný výsledek.

Pro zpracování uživatelských autorizací pomocí příkazu `setmqaut` jsou všechny ekvivalentní následující údaje.

Tabulka 70. Nastavení autorizace uživatele	
Příkaz	Poznámka
<code>setmqaut -m QM -t qmgr -p jodoe +connect</code>	Jedná se o plochý, nekvalifikovaný název, vyřešený prostřednictvím SHORTUSR.
<code>setmqaut -m QM -t qmgr -pJohnDoe1@yourcompany.com +connect</code>	Také plochý, nekvalifikovaný název, který řeší přes USRFIELD na stejnou entitu.
<code>setmqaut -m QM -t qmgr -p email=JohnDoe1@yourcompany.com +connect</code>	Použití pojmenovaného atributu.
<code>setmqaut -m QM -t qmgr -p "phone=1234567" +connect</code>	Použití jiného pojmenovaného atributu, který nemusí být žádným z hodnot nakonfigurovaných na objektu AUTHINFO.

Jako alternativu k příkazu **setmqaut** můžete použít příkaz MQSC `SET AUTHREC` :

```
SET AUTHREC OBJTYPE(QMGR) PRINCIPAL('JohnDoe1@yourcompany.com') AUTHADD(connect)
```

nebo příkaz `Set Authority Record (MQCMD_SET_AUTHRE/REC) PCF` s prvkem `MQCACF_PRINCIP_ENTITY_NAMES`, který obsahuje řetězec:

```
"cn=JohnDoe,ou=users,o=yourcompany,c=yourcountry"
```

Při zpracování skupin se nevyskytuje žádná nejednoznačnost zpracování shortname , protože neexistuje požadavek na přizpůsobení jakékoli formy názvu skupiny do 12 znaků. Proto neexistuje ekvivalent atributu SHORTUSR pro skupiny.

To znamená, že příklady syntaxe popsané v Tabulka 71 na stránce 389 jsou platné, za předpokladu, že jste nakonfigurovali objekt AUTHINFO s rozšířenými atributy a nastavili:

```
GRPFIELD(longname)  
BASEDNG(ou=groups,o=yourcompany,c=yourcountry ) CLASSGRP(groupOfNames)
```

Tabulka 71. Nastavení autorizace skupiny

Příkaz	Poznámka
setmqaut -m QM -t qmgr -g ApplicationGroupA +connect	Použití GRPFIELD k vyřešení
setmqaut -m QM -t qmgr -g longname=ApplicationGroupA +connect	Pojmenování jednoho atributu
setmqaut -m QM -t qmgr -g "cn=Application Group A,ou=groups,o=yourcompany,c=yourcountry" +connect	Použití úplných DN

Jako alternativu k předcházejícímu příkazu **setmqaut** můžete použít příkaz MQSC SET AUTHREC :

```
SET AUTHREC OBJTYPE(QMGR) GROUP('ApplicationGroupA')
AUTHADD(connect)
```

nebo příkaz Set Authority Record (MQCMD\_SET\_AUTHREC) PCF s prvkem MQCACF\_GROUP\_ENTITY\_NAMES obsahujícím řetězec:

```
"ApplicationGroupA"
```

#### Důležité:

Kterýkoli formát, který použijete k odkazování na jméno, ať už pro uživatele nebo skupinu, musí být možné odvodit jedinečné DN.

Takže například nesmíte mít dva různé záznamy, které mají oba "shortu=jodoe".

Pokud nelze určit jednotlivé jedinečné DN, vrátí objekt OAM MQRC\_UNKNOWN\_ENTITY.

## V 8.0.0.2 Zobrazení autorizací

Různé metody zobrazení autorizace uživatelů nebo skupin.

### příkaz dspmqaut

Nejjednodušší metodou zobrazení autorizací dostupných pro uživatele nebo skupinu je použití příkazu dspmqaut .

Pro identifikaci uživatele nebo skupiny můžete použít dotaz na libovolné variace syntaxe. Všimněte si, že výstup příkazu opakuje identitu ve formátu uvedeném na příkazovém řádku. Výstup nehlásí úplný rozlišující název DN.

Příklad:

```
dspmqaut -m QM -t qmgr -p johndoe
Entity johndoe has the following authorizations for object QM:
connect
```

, nebo

```
dspmqaut -m QM -t qmgr -p email=JohnDoe1@yourcompany.com
Entity email=JohnDoe1@yourcompany.com has the following authorizations for object QM:
connect
```

## Příkazy `dmpmqaut` a `dmpmqcfg`

Příkaz `dmpmqaut` a jeho ekvivalenty MQSC nebo PCF mohou určovat činitele nebo skupinu v kterémkoli z podporovaných formátů, jako jsou tabulky `setmqaut` popsané v části “Nastavení oprávnění” na stránce 388. Nicméně, na rozdíl od `dspmqaut`, příkaz `dmpmqaut` vždy nahlásí úplné DN.

```
dmpmqaut -m QM -t qmgr -p jodoe
-----
profile: self
object type: qmgr
entity: cn=JohnDoe, ou=users, o=yourcompany, c=yourcountry
entity type: principal
authority: connect
```

Podobně příkaz `dmpmqcfg`, který nemá žádné filtrování na vybraných záznamech, vždy zobrazí úplné DN ve formátu, který lze přehrát později.

```
dmpmqcfg -m QM -x authrec
-----
SET AUTHREC PROFILE(SELF) +
  PRINCIPAL('cn=JohnDoe, ou=users, o=yourcompany, c=yourcountry') +
  OBJTYPE(QMGR)
  AUTHADD(CONNECT)
```

### V 8.0.0.2 Další pokyny při použití autorizace LDAP

Stručný popis změn rozhraní MQI (Message Queue Interface) a dalších příkazů MQSC a PCF, o kterých byste měli být informováni při použití autorizace LDAP z produktu IBM MQ 8.0.0, opravná sada Fix Pack 2.

#### ADOPTCTX

Nejsou žádné požadavky na aplikace poskytující informace o ověření, nebo pro atribut `ADOPTCTX`, který má být nastaven na hodnotu YES.

Pokud se aplikace explicitně neověřuje, nebo pokud je parametr `ADOPTCTX` nastaven na hodnotu NO pro aktivní objekt `CONNAUTH`, převezme se kontext identity přidružený k aplikaci z ID uživatele operačního systému.

Je-li třeba aplikovat autorizace, tento kontext se namapuje na identitu LDAP pomocí stejných pravidel jako pro příkazy `setmqaut`.

#### Vstupní parametry pro volání MQI

`MQOPEN`, `MQPUT1a` `MQSUB` mají struktury, které umožňují zadat alternativní ID uživatele.

Jsou-li tato pole použita, je 12znakové ID uživatele mapováno na DN pomocí stejných pravidel, jako na příkazech `setmqaut`, `dmpmqaut` a `dspmqaut`.

`MQPUT` a `MQPUT1` také umožňují vhodně autorizovaným programům nastavit pole `MQMD UserIdentifier`. Hodnota tohoto pole nebude během procesu PUT nastavena na police a lze ji nastavit na libovolnou hodnotu.

Jako obvykle však může být hodnota `UserIdentifier` použita pro autorizaci v pozdějších fázích zpracování zpráv, například když je na přijímajícím kanálu definován parametr `PUTAUT (CTX)`.

V tomto okamžiku bude identifikátor zkontrolován kvůli autorizaci pomocí konfigurace přijímajícího správce front-což může být LDAP nebo založeno na technologii OSS.

#### Výstupní parametry pro volání MQI

Kdekoli je ID uživatele poskytnuto programu ve struktuře MQI, je to 12znaková verze krátkého názvu přidružená k připojení.

Například hodnota `MQAXC.UserId` pro rozhraní API Exits je krátký název vrácený z mapování LDAP.

## Další administrativní příkazy MQSC a PCF

Příkazy, které zobrazují informace o uživateli ve stavu objektu, například `DISPLAY CONN USERID`, vracejí 12znakový krátký název přidružený k danému kontextu. Úplné DN se nezobrazí.

Příkazy, které umožňují deklarovat identitu, jako například mapovací pravidla `CHLAUTH` nebo hodnoty `MCAUSER` pro kanály, mohou převzít hodnoty až do maximální délky definované pro tyto atributy (momentálně 64 znaků).

Syntaxe není nijak změněna. Je-li pro tuto identitu požadováno oprávnění, je interně mapováno na DN pomocí stejných pravidel jako pro příkazy `setmqaut`, `dmpmqaut` a `dspmqa`.

To znamená, že hodnota `MCAUSER` v definici kanálu se nemusí zobrazit jako stejný řetězec jako `DISPLAY CHSTATUS`, ale odkazují na stejnou identitu.

Příklad:

```
DEFINE CHL(SV1) CHLTYPE(SVRCONN) MCAUSER('cn=JohnDoe')
DEFINE CHL(SV2) CHLTYPE(SVRCONN) MCAUSER('jodoe')
DEFINE CHL(SV3) CHLTYPE(SVRCONN) MCAUSER('JohnDoe1@yourcompany.com')
```

Pak příkaz `DISPLAY CHSTATUS (*) ALL` zobrazí hodnotu `SHORTUSR`, `MCAUSER` (*jodoe*) pro všechna připojení.

## V 8.0.0.2 Přepínání mezi modely autorizace OS a LDAP

Jak přepínáte mezi různými metodami autorizace na různých platformách.

Atribut `CONNAUTH` pro správce front ukazuje na objekt `AUTHINFO`. Je-li objekt typu `IDPWLDAP`, použije se pro ověření úložiště LDAP.

Nyní můžete použít metodu autorizace pro stejný objekt, který vám umožňuje pokračovat v autorizaci založené na operačním systému, nebo pracovat s autorizací LDAP.

### Platformy UNIX a IBM i

Správce front lze přepínat kdykoli mezi OS a modely LDAP. Konfiguraci můžete změnit a aktivovat ji tak, že použijete příkaz `REFRESH SECURITY TYPE (CONNAUTH)`.

Například, pokud byl tento objekt již nakonfigurován s informacemi o připojení pro ověření:

```
ALTER AUTHINFO(MYLDAP) AUTHTYPE(IDPWLDAP) +
    AUTHORMD(SEARCHGRP) +
    BASEDNG('ou=groups,o=ibm,c=uk') +
    <other attributes>
ALTER QMGR CONNAUTH(MYLDAP)
REFRESH SECURITY
```

### Pravidla zpracování

Když přepínáte z OS na autorizaci LDAP, všechna existující pravidla oprávnění operačního systému, která byla nastavena, se stanou neaktivními a neviditelnými.

Příkazy jako například `dmpmqaut` nezobrazují tato pravidla operačního systému. Podobně při přepnutí z LDAP na OS se všechny definované autorizace LDAP stanou neaktivními a neviditelnými, čímž se obnoví původní pravidla operačního systému.

Chcete-li zálohovat definice správce front z libovolného důvodu pomocí příkazu `dmpmqcfig`, bude tato záloha obsahovat pouze pravidla, která jsou definována pro autorizační metodu v platnosti v době zálohování.

Přehled o tom, jak každá platforma spravuje službu LDAP.

Při použití autorizace LDAP není členství ve skupině `mqm` (nebo ekvivalent) v operačním systému důležité. Členství v této skupině řídí pouze to, zda lze zpracovat určité příkazy příkazového řádku.

Konkrétně musíte být v této skupině, chcete-li vydat příkazy `strmqm` a `endmqm`.

Jakmile je správce front spuštěn, jsou nyní limity na plně privilegovaném účtu. Kromě ID uživatele osoby, která vydává příkaz `strmqm`, jiní uživatelé patřící do skupiny operačního systému `mqm` (nebo ekvivalentní skupiny) nemají speciální oprávnění.

Oprávnění ostatních uživatelů jsou založena na tom, do kterých skupin LDAP patří. Nekvalifikované použití názvu skupiny `mqm` v příkazech, jako například `setmqaut`, není povoleno mapovat na žádnou skupinu LDAP.

### UNIX platformy

Jakmile je správce front spuštěn, jediným automaticky privilegovaným účtem je skutečný uživatel, který spustil správce front.

ID `mqm` stále existuje a používá se jako vlastník prostředků operačního systému, jako jsou například soubory, protože `mqm` je efektivní ID, pod kterým je správce front spuštěn. Uživatel `mqm` však nebude automaticky schopen provádět administrativní úlohy řízené OAM.

### IBM i

V systému IBM i jsou automaticky privilegované účty `ta`, která spouští správce front a ID `QMQM`.

Potřebujete obě ID, protože ID uživatele, které spouští správce front, je nezbytné pouze ke spuštění systému. Jakmile je správce front spuštěn, má pouze oprávnění `QMQM`.

### ukázkový skript

Vzhledem k tomu, že je užitečné mít skupinu schopnou provádět úplnou administraci ve správcích front, je ukázkový skript dodáván na platformách UNIX jako:

```
<install dir>/samp/bin/amqauthg.sh
```

Tato ukázka má dva parametry:

- Název správce front
- Název skupiny LDAP

Ukázkové procesy používají příkazy `setmqaut`, které poskytují úplnou autoritu pro všechny objekty. Jedná se o stejný skript, který je generován průvodcem OAM produktu MQ Explorer pro administrativní role. Například, kód začíná:

```
setmqaut -t q -m <qmgr> -n "*" +alladm +allmqi -g  
<groupname>
```

## Důvěrnost zpráv

Chcete-li zachovat důvěrnost, zašifrujte zprávy. V produktu IBM MQ existují různé metody šifrování zpráv v závislosti na vašich potřebách.

Vaše volba CipherSpec určuje úroveň důvěrnosti, kterou máte.

Pokud potřebujete ochranu dat na úrovni koncových bodů pro vaši dvoubodovou infrastrukturu systému zpráv, můžete použít produkt IBM MQ Advanced Message Security k šifrování zpráv nebo napsat vlastní uživatelskou proceduru rozhraní API nebo uživatelskou proceduru pro přechod na 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 IBM MQ Advanced Message Security naleznete v tématu [“Plánování pro databázi Advanced Message Security”](#) na stránce 90. Použití SSL a TLS s IBM MQ je popsáno v [“Protokoly zabezpečení SSL a TLS v produktu IBM MQ”](#) na stránce 22. Použití ukončovacích programů v šifrování zpráv je popsáno v [“Implementace utajení v uživatelských ukončovacích programech”](#) na stránce 401.

### Související informace

[Připojení dvou správců front s použitím zabezpečení SSL nebo TLS](#)

[Bezpečná připojení klienta ke správci front](#)

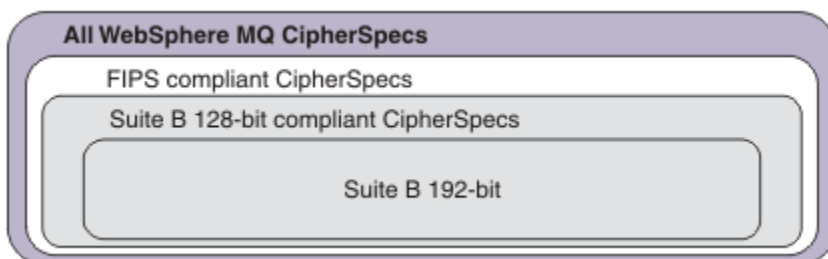
## Povolení specifikace CipherSpecs

Povolte 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 MQ, jsou kompatibilní s FIPS. Některé ze specifikací CipherSpecs standardu FIPS jsou také kompatibilní se sadou Suite B, přestože jiné, například TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (zamítnuto), nejsou.

Všechny kompatibilní specifikace CipherSpecs kompatibilní se standardem Suite B jsou také kompatibilní s FIPS. Všechny specifikace CipherSpecs kompatibilní s Suite B spadají do dvou skupin: 128 bitů (například ECDHE\_ECDSA\_AES\_128\_GCM\_SHA256) a 192 bitů (například ECDHE\_ECDSA\_AES\_256\_GCM\_SHA384),















Následující diagram ilustruje vztah mezi těmito dílčími sadami:



**V 8.0.0.3** Od IBM MQ Verze 8.0.0, opravná sada 3 bylo sníženo počet podporovaných CipherSpecs. Další informace o seznamu podporovaných CipherSpecs a o tom, jak lze povolit zamítnuté CipherSpecs, naleznete v příručce [“Hodnoty CipherSpec podporované v produktu IBM MQ”](#) na stránce 37.

Seznam CipherSpecs, které je třeba znovu povolit pro použití s produktem IBM MQ, naleznete v tématu [“Zamítnuté CipherSpecs”](#) na stránce 396.

Specifikace šifer, které lze použít s správcem front produktu IBM MQ, jsou automaticky uvedeny v následující tabulce. Požadujete-li osobní certifikát, určíte velikost klíče pro dvojici veřejný a soukromý klíč. Velikost klíče, která se použije během navázání komunikace přes zabezpečení SSL, je velikost uložená v certifikátu, pokud není určena CipherSpec, jak je uvedeno v tabulce.

Podpora platformy "1" na stránce 395	Název specifikace šifrování	Použitý protokol	Integrita dat	Šifrovací algoritmus	Šifrování bitů	FIPS "2" na stránce 395	Suite B
   	TLS_RSA_WITH_AES_128_CBC_SHA	TLS 1.0	SHA-1	AES	128	Ano	Ne
   	TLS_RSA_WITH_AES_256_CBC_SHA <sup>"3"</sup> na stránce 395	TLS 1.0	SHA-1	AES	256	Ano	Ne
Vše	ECDHE_ECDSA_AES_128_CBC_SHA256	TLS 1.2	SHA-256	AES	128	Ano	Ne
Vše	ECDHE_ECDSA_AES_256_CBC_SHA384 <sup>"3"</sup> na stránce 395	TLS 1.2	SHA-384	AES	256	Ano	Ne
	ECDHE_ECDSA_AES_128_GCM_SHA256 <sup>"4"</sup> na stránce 395	TLS 1.2	AEAD AES-128 GCM	AES	128	Ano	128bitové
	ECDHE_ECDSA_AES_256_GCM_SHA384 <sup>"3"</sup> na stránce 395 <sup>"4"</sup> na stránce 395	TLS 1.2	AEAD AES-128 GCM	AES	256	Ano	192bitové
Vše	ECDHE_RSA_AES_128_CBC_SHA256	TLS 1.2	SHA-256	AES	128	Ano	Ne
Vše	ECDHE_RSA_AES_256_CBC_SHA384 <sup>"3"</sup> na stránce 395	TLS 1.2	SHA-384	AES	256	Ano	Ne
Vše	ECDHE_RSA_AES_128_GCM_SHA256 <sup>"4"</sup> na stránce 395	TLS 1.2	AEAD AES-128 GCM	AES	128	Ano	Ne
Vše	ECDHE_RSA_AES_256_GCM_SHA384 <sup>"3"</sup> na stránce 395 <sup>"4"</sup> na stránce 395	TLS 1.2	AEAD AES-128 GCM	AES	SHA384	Ano	Ne
 "5" na stránce 395	ECDHE_ECDSA_RC4_128_SHA256	TLS 1.2	AEAD AES-128 GCM	AES	SHA256	Ano	Ne
	ECDHE_ECDSA_3DES_EDE_CBC_SHA256	TLS 1.2	AEAD AES-128 GCM	3DES	SHA256	Ano	Ne
	ECDHE_RSA_3DES_EDE_CBC_SHA256	TLS 1.2	AEAD AES-128 GCM	3DES	SHA256	Ano	Ne
	ECDHE_RSA_RC4_128_SHA256	TLS 1.2	AEAD AES-128 GCM	RSA	SHA256	Ano	Ne

Podpora platformy "1" na stránce 395	Název specifikace šifrování	Použitý protokol	Integrita dat	Šifrovací algoritmus	Šifrování bitů	FIPS "2" na stránce 395	Suite B
IBM i	ECDHE_RSA_NULL_SHA256	TLS 1.2	AEAD AES-128 GCM	RSA	SHA256	Ano	Ne
IBM i	ECDHE_ECDSA_NULL_SHA256	TLS 1.2	AEAD AES-128 GCM	ECDSA	SHA256	Ano	Ne
IBM i	ECDHE_ECDSA_AES_256_GCM_SHA384 "3" na stránce 395 "4" na stránce 395	TLS 1.2	AEAD AES-128 GCM	AES	SHA384	Ano	Ne
z/OS Windows UNIX Linux	TLS_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2	SHA-256	AES	128	Ano	Ne
z/OS Windows UNIX Linux	TLS_RSA_WITH_AES_256_CBC_SHA256 "3" na stránce 395	TLS 1.2	SHA-256	AES	256	Ano	Ne
distributed	TLS_RSA_WITH_AES_128_GCM_SHA256 "4" na stránce 395	TLS 1.2	AEAD AES-128 GCM	AES	128	Ano	Ne
distributed	TLS_RSA_WITH_AES_256_GCM_SHA384 "3" na stránce 395 "4" na stránce 395	TLS 1.2	AEAD AES-128 GCM	AES	256	Ano	Ne

#### 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. Tuto specifikaci šifrování nelze použít k zabezpečení připojení z produktu MQ Explorer na správce front, pokud nebudou v prostředí JRE průzkumníkem Explorer použity příslušné soubory neomezených zásad.
4. Dle doporučení NIST mají specifikace šifrování GCM omezení, což znamená, že po odeslání  $2^{32}$  TLS záznamů pomocí jednoho klíče relace se připojení ukončí se zprávou AMQ9288.

Chcete-li zabránit výskytu této chyby, vyhněte se použití šifer GCM, povolte reset tajného klíče, nebo spusťte správce front IBM MQ s proměnnou prostředí `GSK_ENFORCE_GCM_RESTRICTION=GSK_FALSE`.

**Důležité:** Omezení GCM je aktivní, bez ohledu na použitý režim FIPS.

5. Specifikace šifrování CipherSpecs, která je uvedena jako podpora v systému IBM i, platí pro verze 7.2 a 7.3 systému IBM i.

#### Související pojmy

["Digitální certifikáty a kompatibilita CipherSpec v produktu IBM MQ" na stránce 44](#)

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 MQ.



## Související informace

Definovat kanál















ZMĚNIT KANÁL

## Zamítnuté CipherSpecs

Seznam zamítnutých CipherSpecs, který je v případě potřeby schopen použít s produktem IBM MQ.

Další informace o tom, jak lze povolit zamítnuté CipherSpecs, naleznete v příručce [“Hodnoty CipherSpec podporované v produktu IBM MQ”](#) na stránce 37.

Zamítnuté CipherSpecs, které můžete použít s podporou zabezpečení IBM MQ TLS a SSL, jsou vypsány v následující tabulce.

Podpora platformy “1” na stránce 398	Název specifikace šifrování	Použitý protokol	Integrita dat	Šifrovací algoritmus	Šifrování bitů	FIPS “2” na stránce 398	Suite B	Aktualizovat při zamítnutí
	AES_SHA_US	SSL 3.0	SHA-1	AES	128	Ne	Ne	8.0.0.2
Vše	DES_SHA_EXPORT <sup>“3”</sup> na stránce 398 <sup>“8”</sup> na stránce 398	SSL 3.0	SHA-1	DES	56	Ne	Ne	8.0.0.2
  	DES_SHA_EXPORT1024 <sup>“4”</sup> na stránce 398	SSL 3.0	SHA-1	DES	56	Ne	Ne	8.0.0.2
  	FIPS_WITH_DES_CBC_SHA	SSL 3.0	SHA-1	DES	56	Ne <sup>“6”</sup> na stránce 398	Ne	8.0.0.2
  	FIPS_WITH_3DES_EDE_CBC_SHA	SSL 3.0	SHA-1	3DES	168	Ne <sup>“7”</sup> na stránce 398	Ne	8.0.0.6
Vše	NULL_MD5	SSL 3.0	MD5	Není	0	Ne	Ne	8.0.0.2
Vše	NULL_SHA	SSL 3.0	SHA-1	Není	0	Ne	Ne	8.0.0.2
Vše	RC2_MD5_EXPORT <sup>“3”</sup> na stránce 398 <sup>“8”</sup> na stránce 398	SSL 3.0	MD5	RC2	40	Ne	Ne	8.0.0.3
Vše	RC4_MD5_EXPORT <sup>“3”</sup> na stránce 398	SSL 3.0	MD5	RC4	40	Ne	Ne	8.0.0.3
Vše	RC4_MD5_US	SSL 3.0	MD5	RC4	128	Ne	Ne	8.0.0.3
Vše	RC4_SHA_US <sup>“8”</sup> na stránce 398	SSL 3.0	SHA-1	RC4	128	Ne	Ne	8.0.0.3
  	RC4_56_SHA_EXPORT1024 <sup>“4”</sup> na stránce 398	SSL 3.0	SHA-1	RC4	56	Ne	Ne	8.0.0.3
Vše	TRIPLE_DES_SHA_US <sup>“8”</sup> na stránce 398	SSL 3.0	SHA-1	3DES	168	Ne	Ne	8.0.0.6
	TLS_RSA_EXPORT_WITH_RC2_40_MD5	TLS 1.0	MD5	RC2	40	Ne	Ne	8.0.0.3

Podpora platformy "1" na stránce 398	Název specifikace šifrování	Použitý protokol	Integrita dat	Šifrovací algoritmus	Šifrování bitů	FIPS "2" na stránce 398	Suite B	Aktualizovat při zamítnutí
IBM i	TLS_RSA_EXPORT_WITH_RC4_40_MD5 <sup>"3"</sup> na stránce 398	TLS 1.0	MD5	RC4	40	Ne	Ne	8.0.0.3
Vše	TLS_RSA_WITH_DES_CBC_SHA	TLS 1.0	SHA-1	DES	56	Ne <sup>"5"</sup> na stránce 398	Ne	8.0.0.2
IBM i	TLS_RSA_WITH_NULL_MD5	TLS 1.0	MD5	Není	0	Ne	Ne	8.0.0.2
IBM i	TLS_RSA_WITH_NULL_SHA	TLS 1.0	SHA-1	Není	0	Ne	Ne	8.0.0.2
IBM i	TLS_RSA_WITH_RC4_128_MD5	TLS 1.0	MD5	RC4	128	Ne	Ne	8.0.0.3
Windows UNIX Linux	ECDHE_ECDSA_NULL_SHA256	TLS 1.2	SHA-1	Není	0	Ne	Ne	8.0.0.2
Windows UNIX Linux	ECDHE_ECDSA_RC4_128_SHA256	TLS 1.2	SHA-1	RC4	128	Ne	Ne	8.0.0.3
Windows UNIX Linux	ECDHE_RSA_NULL_SHA256	TLS 1.2	SHA-1	Není	0	Ne	Ne	8.0.0.2
Windows UNIX Linux	ECDHE_RSA_RC4_128_SHA256	TLS 1.2	SHA-1	RC4	128	Ne	Ne	8.0.0.3
Windows UNIX Linux	TLS_RSA_WITH_NULL_NULL	TLS 1.2	Není	Není	0	Ne	Ne	8.0.0.2
Vše	TLS_RSA_WITH_NULL_SHA256	TLS 1.2	SHA-256	Není	0	Ne	Ne	8.0.0.3
Windows UNIX Linux	TLS_RSA_WITH_RC4_128_SHA256	TLS 1.2	SHA-1	RC4	128	Ne	Ne	8.0.0.3
Vše	TLS_RSA_WITH_3DES_EDE_CBC_SHA <sup>"9"</sup> na stránce 398	TLS 1.0	SHA-1	3DES	168	Ano	Ne	8.0.0.6
Windows UNIX Linux	ECDHE_ECDSA_3DES_EDE_CBC_SHA256 <sup>"9"</sup> na stránce 398	TLS 1.2	SHA-1	3DES	168	Ano	Ne	8.0.0.6
Windows UNIX Linux	ECDHE_RSA_3DES_EDE_CBC_SHA256 <sup>"9"</sup> na stránce 398	TLS 1.2	SHA-1	3DES	168	Ano	Ne	8.0.0.6

Podpora platformy "1" na stránce 398	Název specifikace šifrování	Použitý protokol	Integrita dat	Šifrovací algoritmus	Šifrování bitů	FIPS "2" na stránce 398	Suite B	Aktualizovat při zamítnutí
--------------------------------------	-----------------------------	------------------	---------------	----------------------	----------------	-------------------------	---------	----------------------------

**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. Tyto specifikace šifrování již produkt IBM MQ classes for Java nebo IBM MQ classes for JMS nepodporuje. Další informace viz [Specifikace šifrování a šifrovací sady SSL/TLS v produktu IBM MQ classes for Java](#) nebo [Specifikace šifrování a šifrovací sady SSL/TLS v produktu IBM MQ classes for JMS](#).
9. 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.

**Související pojmy**

[“Digitální certifikáty a kompatibilita CipherSpec v produktu IBM MQ” na stránce 44](#)

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 MQ.

**Související informace**

[Definovat kanál](#)

[ZMĚNIT KANÁL](#)

**Získání informací o produktu CipherSpecs pomocí Průzkumníka IBM MQ**

Produkt IBM MQ Explorer můžete použít k zobrazení popisů CipherSpecs.

Chcete-li získat informace o CipherSpecs v produktu [“Povolení specifikace CipherSpecs” na stránce 393](#), postupujte takto:

1. Otevřete produkt **IBM MQ Explorer** a rozbalte složku **Správci front** .
2. Ujistěte se, že jste spustili správce front.
3. Vyberte správce front, se kterým chcete pracovat, a klepněte na **Kanály**.
4. Klepněte pravým tlačítkem myši na kanál, se kterým chcete pracovat, a vyberte **Vlastnosti**.
5. Vyberte stránku vlastností **SSL** .
6. Vyberte ze seznamu CipherSpec , se kterou chcete pracovat. Popis se zobrazí v okně pod seznamem.

## 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 IBM MQ, takže nové specifikace 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 “[Povolení specifikace CipherSpecs](#)” na stránce 393. 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 najdete v příslušné dokumentaci k produktu (vyhledejte *cipher\_spec*):

- Pro V5R3, [dokumentace k produktu iSeries](#)
- Pro V5R4, [dokumentace 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

Four-znakový řetězec reprezentující hexadecimální hodnotu. Hexadecimální kódy odpovídají hodnotám definovaným v protokolu SSL.

Další informace naleznete v tématu [Definice šifrovacích sad](#), kde je uveden seznam všech podporovaných specifikací šifer TLS 1.0, TLS 1.2 a TLS 1.3 ve formátu 4místných hexadecimálních kódů.

## Aspekty pro klastry IBM MQ

S klastry produktu IBM MQ je nejbezpečnější použít názvy CipherSpec v produktu “[Povolení specifikace CipherSpecs](#)” na stránce 393. 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 408.

## Určení CipherSpec pro IBM MQ MQI client

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

Jedná se o následující volby:

- Použití tabulky definic kanálů
- Použití pole [SSLCipherSpec](#) ve struktuře MQCD, v MQCD\_VERSION\_7 nebo vyšší, na volání MQCONN.
- Použití Active Directory (na systémech Windows s podporou Active Directory)

## Určení sady CipherSuite s IBM MQ classes for Java a IBM MQ classes for JMS

IBM MQ classes for Java a IBM MQ classes for JMS specifikujte CipherSuites jinak než u jiných platform.

Další informace o určení sady CipherSuite s produktem IBM MQ classes for Javaznajete v tématu [Podpora zabezpečení SSL \(Secure Sockets Layer\) pro produkt Java](#).

Informace o určení sady CipherSuite s produktem IBM MQ classes for JMS naleznete v tématu [Použití zabezpečení SSL \(Secure Sockets Layer\) s produktem IBM MQ classes for JMS](#).

## Určení CipherSpec pro IBM MQ.NET

Pro produkt IBM MQ.NET můžete určit volbu CipherSpec buď pomocí třídy MQEnvironment, nebo pomocí vlastnosti MQC.SSL\_CIPHER\_SPEC\_PROPERTY v hašovací tabulce vlastností připojení.

Informace o určení CipherSpec pro nespravovaného klienta .NET naleznete v tématu [Povolení zabezpečení SSL pro nespravovaného klienta .NET](#) .

Informace o specifikaci CipherSpec pro spravovaného klienta produktu .NET naleznete v tématu [PodporaCipherSpec pro spravovaného klienta .NET](#) .

## Resetování tajných klíčů SSL a TLS

IBM 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 straně kanálu produktu IBM MQ .

### Správce front

Pro správce front použijte příkaz **ALTER QMGR** s parametrem **SSLRKEYC** k nastavení hodnot použitých během nového vyjednávání klíče.

 V systému IBM i použijte parametr **CHGMQM** s argumentem **SSLRSTCNT** .

### 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 struktury MQSCO na volání MQCONN
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 resetování 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 vyjednan 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 MQ classes for Javamůže aplikace resetovat tajný klíč jedním z následujících způsobů:

- Nastavením pole Počet sslResetve tříd 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 konstrukturu.

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 IBM MQ classes for Java před opětovným vyjednáním tajného klíče. Počet odeslaných bajtů je číslo před šifrováním a počet přijatých bajtů je číslo po dešifrování. Počet bajtů také obsahuje řídicí informace odeslané a přijaté klientem IBM MQ classes for 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 IBM MQ classes for JMS představuje 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 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

U nespravovaných klientů .NET udává celočíselné vlastnosti SSLKeyResetpočet nešifrovaných bajtů odeslaných a přijatých v rámci konverzace SSL nebo TLS, než bude znovu vyjednán tajný klíč.

Informace o použití vlastností objektu v produktu IBM MQ classes for .NET naleznete v tématu [Získání a nastavení hodnot atributu](#).

U spravovaných klientů .NET nepodporuje třída SSLStream tajný klíč/opakované domlouvání. However, to be consistent with other IBM MQ clients, the IBM MQ managed .NET client allows applications to set SSLKeyResetCount. Další informace viz téma [Resetování tajného klíče nebo opětovné domlouvání](#).

## XMS .NET

V případě nespravovaných klientů XMS .NET viz [Zabezpečená připojení ke správci front IBM WebSphere MQ](#).

### Související informace

[ZMĚNIT QMGR](#)

[ZOBRAZIT QMGR](#)

Změna správce front zpráv (CHGMQM)

Zobrazení správce front zpráv (DSPMQM)

## Implementace utajení v uživatelských ukončovacích programech

## Implementace utajení v uživatelských procedurách zabezpečení

Uživatelské procedury zabezpečení mohou hrát roli ve službě důvěrnosti tím, že generují a distribuují symetrický klíč pro šifrování a dešifrování dat, která proudí na kanál. Běžnou technikou pro to je využití technologie PKI.

Jedna uživatelská procedura zabezpečení vygeneruje náhodnou datovou hodnotu, zašifruje ji pomocí veřejného klíče správce front nebo uživatele, který zástupce pro zabezpečení partnera reprezentuje, a odešle zašifrovaná data svému partnerovi do zprávy zabezpečení. Partner pro zabezpečení ochrany dat dešifruje náhodná hodnota 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 401.

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 příjem 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 druhých 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. Pokud používáte produkt IBM MQ Advanced Message Service (AMS), můžete uvést integritu pro jedinečnou zprávu.

#### Implementace integrity dat ve výstupních procedurách zpráv

Zpráva může být digitálně podepsána ukončením zprávy na odesílajícím konci kanálu. Digitální podpis lze poté zkontrolovat uživatelskou procedurou na přijímajícím konci kanálu a zjistit, zda byla zpráva záměrně upravena.

Určitá ochrana může být poskytnuta použitím kódu digest zprávy místo digitálního podpisu. Kód digest zprávy může být účinný proti náhodnému nebo nevybíravému falšování, ale nezabrání tomu, aby byl informovanější jednotlivec měněn nebo nahrazován zprávou a generování zcela nového kódu digest pro tuto zprávu. To platí zejména v případě, že algoritmus používaný ke generování kódu digest zprávy je dobře známý.

#### Implementace integrity dat v uživatelských procedurách odesílání a příjmu

Na kanálu zpráv jsou uživatelské procedury pro poskytování této služby vhodnější, protože uživatelská procedura pro zprávy má přístup k celé zprávě. Na kanálu MQI mohou parametry volání MQI obsahovat data aplikace, která je třeba chránit, a tuto ochranu může poskytnout pouze odeslání a přijetí uživatelských procedur.

#### Implementace integrity dat v uživatelské proceduře rozhraní API nebo ukončení přeletu rozhraní API

Zprávu lze digitálně podepsat pomocí rozhraní API nebo předání rozhraní API, když je zpráva vložena odesílající aplikací. Digitální podpis pak může být zkontrolován druhou uživatelskou procedurou, když je zpráva načtena přijímající aplikací za účelem zjištění, zda byla zpráva úmyslně upravena.

Určitá ochrana může být poskytnuta použitím kódu digest zprávy místo digitálního podpisu. Kód digest zprávy může být účinný proti náhodnému nebo nevybíravému falšování, ale nezabrání tomu, aby byl informovanější jednotlivec měněn nebo nahrazován zprávou a generování zcela nového kódu digest pro tuto zprávu. To platí zejména v případě, že algoritmus používaný ke generování kódu digest zprávy je dobře známý.

### Další informace

Další informace o zajištění integrity dat naleznete v části [“Povolení specifikace CipherSpecs”](#) na stránce 393.

#### Související informace

[Připojení dvou správců front s použitím zabezpečení SSL nebo TLS](#)

[Bezpečná připojení klienta ke správci front](#)

## Auditování

---

Můžete zkontrolovat narušení zabezpečení nebo pokusy o narušení pomocí zpráv událostí. Zabezpečení vašeho systému můžete také zkontrolovat pomocí 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 správčům front připojícím 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 správčům 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 správčům 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 umísťují zprávy do vašich front. Autorizujte vzdáleného správce front tím, že zkontrolujete ID uživatele ve zprávě pomocí produktu RACF v systému z/OS nebo na OAM na jiných platformách.

#### Informace o této úloze

K řízení přístupu k frontám slouží bezpečnostní zařízení platformy a mechanismus řízení přístupu v produktu IBM MQ .

#### Postup

1. Chcete-li zabránit určitým správčům front ve vkládání zpráv do fronty, použijte nástroje zabezpečení, které jsou k dispozici na vaší platformě.

Příklad:

- RACF nebo další externí správci zabezpečení v systému IBM MQ for z/OS
  - Správce oprávnění k objektu (OAM) na jiných platformách.
2. Použijte příkaz put, PUTAUT, atribut na definici kanálu CLUSRCVR .

Atribut PUTAUT vám umožňuje uvést, jaké identifikátory uživatelů se mají použít k zavedení oprávnění pro vložení zprávy do fronty.

Volby v atributu PUTAUT jsou:

#### **DEF**

Použijte výchozí ID uživatele. V systému z/OS může kontrola zahrnovat použití ID uživatele přijatého ze sítě a odvozeného od uživatele MCAUSER.

#### **CTX**

Použijte ID uživatele v kontextových informacích přidružených ke zprávě. V systému z/OS se kontrola může týkat buď použití ID uživatele přijatého ze sítě, nebo odvozeného od uživatele MCAUSER, nebo obou. Tuto volbu použijte, je-li odkaz důvěryhodný a ověřený.

#### **ONLYMCA (pouze z/OS)**

Co se týká DEF, ale žádné ID uživatele přijaté ze sítě se nepoužívá. Tuto volbu použijte v případě, že odkaz není důvěryhodný. Chcete povolit pouze specifickou sadu akcí na ní, které jsou definovány pro MCAUSER.

#### **ALTMCA (pouze z/OS)**

Co se týče CTX, ale žádné ID uživatele přijaté ze sítě se nepoužije.

## **Autorizace vkládání zpráv ve vzdálených frontách klastru**

V produktu z/OS nastavte autorizaci pro vložení do fronty klastru pomocí produktu RACF. Na jiných platformách autorizujte přístup pro připojení ke správcům front a k jejich vložení do front v těchto správcích front.

### **Informace o této úloze**

Výchozí chování je provádět řízení přístupu vůči serveru SYSTEM.CLUSTER.TRANSMIT.QUEUE. Všimněte si, že toto chování platí i v případě, že používáte více přenosových front.

Specifické chování popsané v tomto tématu platí pouze v případě, že jste konfigurovali atribut **ClusterQueueAccessControl** v souboru `qm.ini` na hodnotu `RQMName`, jak je popsáno v tématu [Sekce zabezpečení](#), a restartováním správce front.

### **Procedura**

- Pro z/OS zadejte následující příkazy:

```
RDEFINE MQQUEUE QMgrName.QUEUE. QueueName UACC(NONE)
PERMIT QMgrName.QUEUE. QueueName CLASS(MQADMIN) ID(GroupName) ACCESS(UPDATE)
```

- 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
```

- Pro IBM izadejte následující příkazy:

```
GRTMQMAUT OBJ(' QMgrName ') OBJTYPE(*MQM) USER(GroupName) AUT(*CONNECT)
GRTMQMAUT OBJ(' QueueName ') OBJTYPE(*Q) USER(GroupName) AUT(*PUT) MQMNAME(' QMgrName ')
```

Uživatel může vkládat zprávy pouze do určené fronty klastru a žádné další fronty klastru.

Názvy proměnných mají následující význam:

#### **QMgrName**

Název správce front. V systému z/OS může být tato hodnota také názvem skupiny sdílení front.

#### **GroupName**

Název skupiny, ke které má být udělen přístup.

## QueueName

Název fronty nebo generický profil, pro který mají být změněna autorizace.

## Jak pokračovat dále

Uvedete-li frontu pro odpověď při vložení zprávy do fronty klastru, musí mít přijímající aplikace oprávnění k odeslání odpovědi. Nastavte toto oprávnění podle pokynů v části [“Udělení oprávnění pro vkládání zpráv do vzdálené fronty klastru”](#) na stránce 373.

## 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 zabráni 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 `MQCPX` 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 navrhuje jako odesílatele, může neautorizovaný správce front bez ukončení zabezpečení vstoupit do klastru, protože se neprovedou žádné kontroly zabezpečení.  
Ne, dokud nebude kanál zastaven a restartován může být název `SCYEXIT` odeslán z definice příjemce klastru a všech provedených kontrol zabezpečení.
5. Chcete-li zobrazit definici odesílacího kanálu klastru, která je aktuálně používána, použijte příkaz:

```
DISPLAY CLUSQMgr( queue manager ) ALL
```

Příkaz zobrazí atributy, které byly odeslány z definice příjemce klastru.

6. Chcete-li zobrazit původní definici, použijte příkaz:

```
DISPLAY CHANNEL( channel name ) ALL
```

7. Možná budete muset definovat uživatelskou proceduru automatické definice kanálu, CHADEXIT, na správci front odesílatele klastru, pokud jsou správci front na různých platformách.

Pomocí uživatelské procedury automatické definice kanálu nastavte atribut SecurityExit na vhodný formát pro cílovou platformu.

8. Proveďte implementaci a konfiguraci zabezpečení.

**z/OS** **z/OS**

Modul načtení uživatelské procedury zabezpečení musí být v datové sadě určené v příkazu CSQXLIB DD procedury adresního prostoru iniciátoru kanálu.

**Windows** **Linux** **UNIX** **Windows, systémy SYSTÉM UNIX a 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 správci front

Vynutí, aby nežádoucí správce front opustil klastr vyvoláním příkazu RESET CLUSTER ve správci front úplného úložiště.

### Informace o této úloze

Můžete vynutit, aby nechtěný správce front opustil klastr. Je-li například odstraněn správce front, avšak jeho kanály příjemce klastru jsou stále definovány v klastru. Možná byste se měl uklidit.

Pouze správci front úplného úložiště mají oprávnění k odebrání správce front z klastru.

**Poznámka:** Přestože použití příkazu RESET CLUSTER vynuceně odebere správce front z klastru, použití příkazu RESET CLUSTER samo o sobě nezabrání opětovnému připojení správce front ke klastru později. Chcete-li se ujistit, že se správce front znovu nepřipojí ke klastru, postupujte podle kroků podrobně uvedených v tématu [“Zabránění připojování správců front ke klastru”](#) na stránce 406.

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 definice lokálních klastrů se zobrazují, aby byly v klastru. Definice ve všech ostatních správci 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 SSL a TLS viz [“Protokoly zabezpečení SSL a TLS v produktu IBM MQ”](#) na stránce 22. Doporučení je obecně použitelné pro kanály klastru, ale možná byste měli věnovat zvláštní pozornost následujícím:

V klastru IBM MQ je určitá definice kanálu CLUSRCVR často šířena do mnoha dalších správců front, kde je transformován na automaticky definované CLUSSDR. Následně se automaticky nadefinovaný CLUSSDR používá ke spuštění kanálu pro CLUSRCVR. Je-li 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 MQ Development a všechny mají společné názvy ve tvaru DEVT.QMnnn, kde nnn je číselný.

V tomto případě hodnota SSLPEER na hodnotě C=UK, O=IBM, OU=IBM MQ Development, CN=DEVT.QM\* na serveru CLUSRCVR umožní úspěšné připojení všech požadovaných odesílacích kanálů klastru, ale zabrání tomu, aby se nechtěné odesílací kanály klastru připojovaly.

- Pokud jsou použity vlastní řetězce CipherSpec, mějte na paměti, že vlastní formáty řetězců nejsou povoleny na všech platformách. Příklad toho je, že řetězec CipherSpec RC4\_SHA\_US má hodnotu 05 na IBM i, ale není platnou specifikací v systémech UNIX, Linux nebo Windows. Pokud se tedy v produktu CLUSRCVR používají 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 klustr, 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 CipherSpecs mohou být nové ve stávajícím vydání produktu IBM MQ a nejsou podporovány ve starších verzích. Klaster obsahující správce front, kteří jsou spuštěni v různých vydáních produktu MQ , mohou používat pouze specifikace CipherSpecs podporované jednotlivými verzemi.

Chcete-li použít novou položku CipherSpec v rámci klastru, musíte nejprve migrovat všechny správce front klastru do aktuální verze.

- Některé specifikace CipherSpecs vyžadují použití specifického typu digitálního certifikátu, zejména těch, které používají komponentu Elliptic Curve Cryptography.



**Upozornění:** Ve správci front, které chcete spojit jako součást klastru, nelze použít směs podepsaných certifikátů Elliptic Curve-podepsaných správců front a certifikátů podepsaných společností RSA.

Správci front v klastru musí používat všechny certifikáty podepsané RSA nebo všechny certifikáty podepsané EC, nikoli směs obou těchto certifikátů.

Další informace viz [“Digitální certifikáty a kompatibilita CipherSpec v produktu IBM MQ”](#) na stránce 44.

Provedte upgrade všech správců front v klastru na IBM MQ V6 nebo vyšší, pokud tyto úrovně ještě nejsou na těchto úrovních. Distribuuje certifikáty a klíče tak, aby SSL fungovalo z každého z nich.

### Informace o této úloze

Změňte kanály CLUSRCVR před kanály CLUSSDR .

### Postup

1. Přepněte kanály CLUSRCVR na zabezpečení SSL v libovolném pořadí, v jakém chcete, při změně jedné hodnoty CLUSRCVR a umožněte, aby se změny v klastru procházela, než se změní další.

**Důležité:** Ujistěte se, že jste nezměnili opačnou cestu, dokud nejsou změny pro aktuální kanál distribuovány po celém klastru.

2. Volitelné: Přepněte všechny ruční kanály CLUSSDR na SSL.

To nemá žádný vliv na činnost klastru, pokud nepoužijete příkaz `REFRESH CLUSTER` s volbou `REPOS(YES)` .

**Poznámka:** Pro velké klastery může být použit příkaz **REFRESH CLUSTER** pro klastr rušivé, zatímco probíhá, a poté znovu ve 27. denních intervalech, když objekty klastru automaticky odesílají aktualizace stavu všem zúčastněným správci front. Viz téma [Aktualizace velkých klastrů mohou ovlivnit jejich výkon a dostupnost](#).

3. Použijte příkaz `DISPLAY CLUSQMGR` , abyste se ujistili, že nová konfigurace zabezpečení byla šířena v celém klastru.
4. Restartujte kanály pro použití zabezpečení SSL nebo TLS a spusťte příkaz `REFRESH SECURITY (SSL)`.

### Související pojmy

[“Povolení specifikace CipherSpecs”](#) na stránce 393

Povolte CipherSpec pomocí parametru **SSLCIPH** buď v příkazu **DEFINE CHANNEL MQSC**, nebo v příkazu **ALTER CHANNEL MQSC**.

“Digitální certifikáty a kompatibilita CipherSpec v produktu IBM MQ” na stránce 44

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 MQ.

### Související informace

Klastrování: [Využití doporučených postupů pro příkaz REFRESH CLUSTER](#)

## Zakázání zabezpečení 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

 nebo \*NONE na IBM i .

Můžete vypnout TLS na přijímacích kanálech klastru v libovolném pořadí, které chcete.

Všimněte si, že změny proudí v opačném směru přes kanály, na kterých jste aktivují TLS.

2. Zkontrolujte, zda se nová hodnota odrazí ve všech ostatních správcích front, pomocí příkazu **DISPLAY CLUSQMGR(\*) ALL**.

3. Vypněte TLS na všech ručních kanálech odesílatele klastru.

To nemá žádný vliv na činnost klastru, pokud nepoužijete příkaz **REFRESH CLUSTER** s volbou REPOS (YES) .

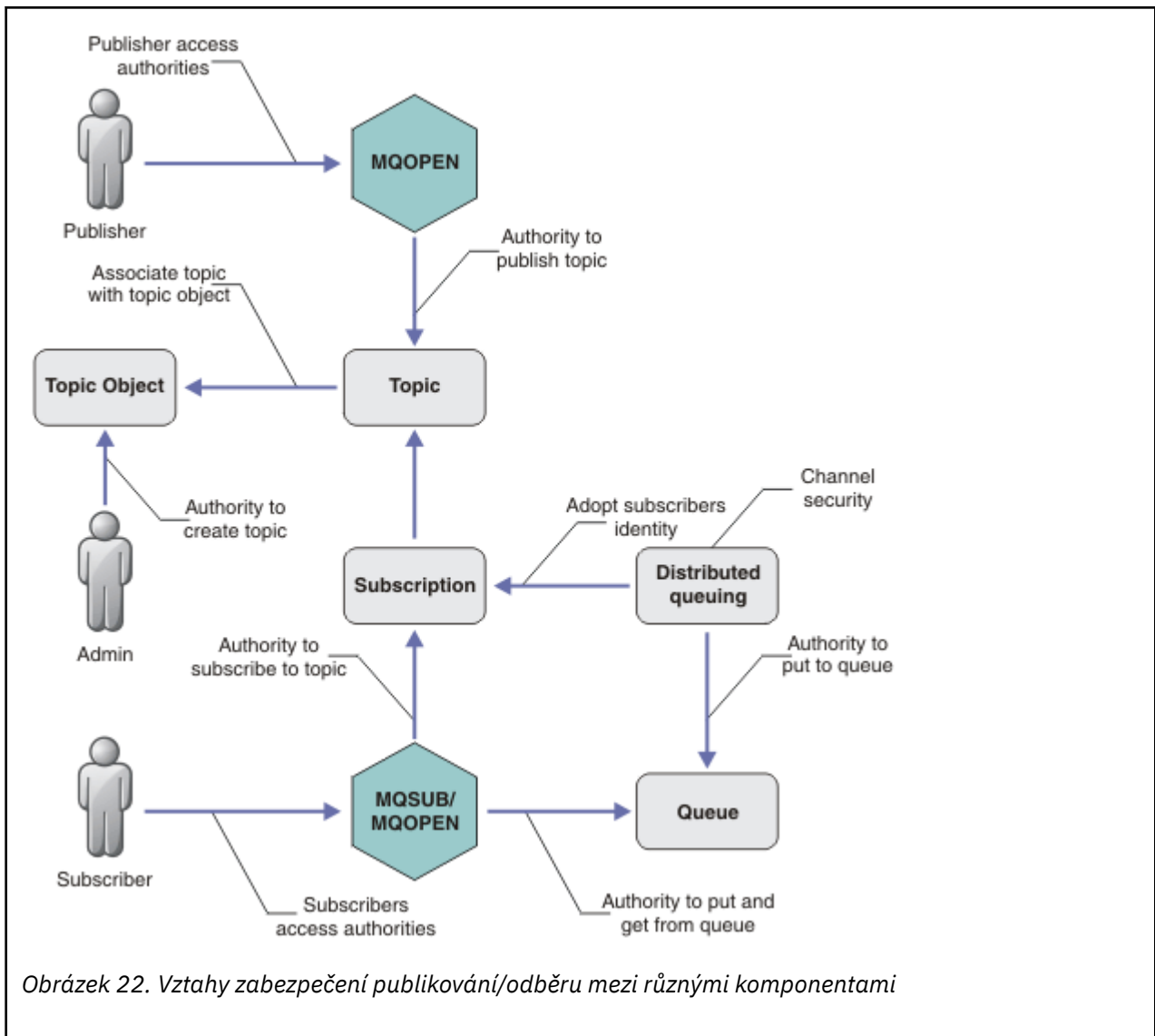
Pro velké klastry může být použití příkazu **REFRESH CLUSTER** pro klastr rušivé, zatímco probíhá jeho zpracování, a poté v pravidelných intervalech, kdy objekty klastru automaticky odesílají aktualizace stavu všem zúčastněným správcům front. Další informace viz [Aktualizace ve velkém klastru může ovlivnit výkon a dostupnost klastru](#) .

4. Zastavte a restartujte odesílací kanály klastru.

## Zabezpečení publikování/odběru

Komponenty a interakce, které se účastní publikování/odběru, jsou popsány jako úvod do podrobnějších vysvětlení a příkladů, které následují.


Existuje celá řada komponent, které se podílejí na publikování a přihlášení k odběru tématu. Některé ze vztahů zabezpečení mezi nimi jsou ilustrovány v [Obrázek 22 na stránce 411](#) a popsány v následujícím příkladu.



### Témata

Témata jsou identifikována pomocí řetězců témat a jsou zpravidla uspořádána do stromů, viz téma [Stromy témat](#). Chcete-li řídit přístup k tématu, je třeba asociovat téma s objektem tématu. Část “Model zabezpečení témat” na stránce 413 vysvětluje, jak zabezpečit témata pomocí objektů témat.

### Objekty administrativního tématu

Můžete určovat, kdo má přístup k tématu, a za jakým účelem můžete použít příkaz **setmqaut** se seznamem objektů administrativních témat. Viz příklady, [“Udělit uživateli přístup k odběru tématu”](#) na stránce 417 a [“Udělit přístup uživateli k publikování v rámci tématu”](#) na stránce 425.  Chcete-li řídit přístup k objektům tématu v systému z/OS, prostudujte si téma [Profily pro zabezpečení témat](#).

### Odběry

Přihlaste se k odběru jednoho nebo více témat tak, že vytvoříte odběr dodávající řetězec tématu, který může obsahovat zástupné znaky, aby se shodovaly s řetězcí témat v publikacích. Další podrobnosti viz:

#### Přihlásit se k odběru pomocí objektu tématu

[“Přihlášení k odběru pomocí názvu objektu tématu”](#) na stránce 414

#### Přihlásit se k odběru pomocí tématu

[“Přihlášení k odběru pomocí řetězce tématu, ve kterém uzel tématu neexistuje”](#) na stránce 415



## **Přihlásit se k odběru tématu se zástupnými znaky**

“Přihlášení k odběru pomocí řetězce tématu, který obsahuje zástupné znaky” na stránce 415

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 430.

## **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 415.

K dispozici nejsou žádné aliasy objektu tématu, ale jako alias pro objekt tématu můžete použít alias fronty. Pokud tak učiníte a kontrolujete oprávnění k používání tématu pro publikování nebo odběr, zkontroluje správce front oprávnění k použití této fronty.

## **“Zabezpečení publikování/odběru mezi správci front” na stránce 432**

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 IBM MQ jsou kanály konfigurovány s použitím PUTAUT = DEF umísťují 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.

Část “Zabezpečení publikování/odběru mezi správci front” na stránce 432 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 vytvoříte nebo obnovíte odběr.

Bez ohledu na to, jakou výzvu použijete, správce front zkontroluje, zda se můžete přihlásit k odběru tématu a získat výsledné publikace z cílové fronty. Je-li cílová fronta nespravovaná, kontroly autorizace jsou také provedeny tak, aby správce front mohl umisťovat publikace do cílové fronty. Používá identitu, kterou přijal z odpovídajícího odběru. Předpokládá se, že správce front je vždy schopen umisťovat publikování do spravovaných cílových front.

## Role

Uživatelé jsou zapojeni do čtyř rolí ve spuštěných aplikacích publikování/odběru:

1. Vydavatel
2. Odběratel
3. Administrátor témat
4. IBM MQ Administrátor-člen skupiny mqm

Definujte skupiny s odpovídajícími autorizacemi, které odpovídají rolím pro publikování, odběr a administraci témat. Poté můžete přiřadit činitele k těmto skupinám, které je opravňují k provedení specifických úloh publikování a odběru.

Kromě toho je třeba rozšířit oprávnění administrativních operací na administrátora front a kanálů zodpovědných za přesun publikací a odběrů.

## Model zabezpečení témat

Přidružené atributy zabezpečení mohou mít pouze definované objekty témat. Popis objektů témat naleznete v tématu [Objekty administrativního tématu](#). Atributy zabezpečení určují, zda má být zadané ID uživatele nebo skupina zabezpečení povoleno provádět odběr nebo operaci publikování pro každý objekt tématu.

Atributy zabezpečení jsou přidruženy k příslušnému uzlu administrace ve stromu témat. Je-li během operace odběru nebo publikování provedena kontrola oprávnění pro určité ID uživatele, je udělené oprávnění založeno na attributech 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.

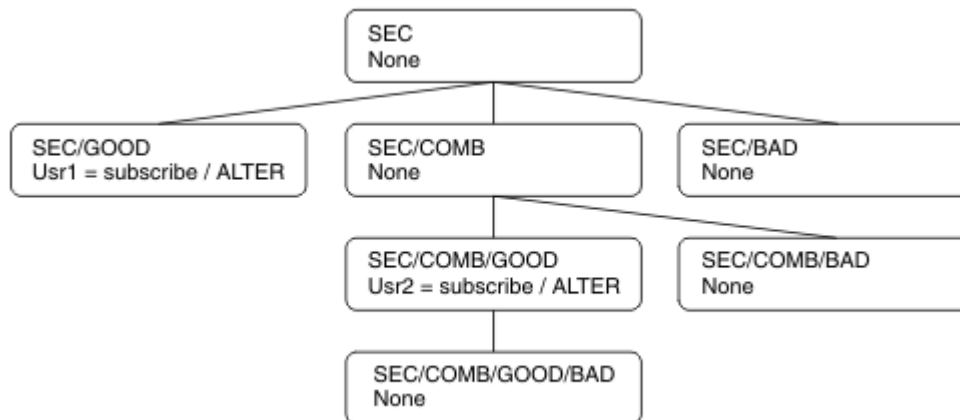
Prohlédněte si následující příklad, kde byly objekty tématu definovány s atributy zabezpečení, nebo s zobrazenými oprávněními:

<i>Tabulka 72. Příklad oprávnění k objektu tématu</i>			
<b>Název tématu</b>	<b>Řetězec tématu</b>	<b>Oprávnění-ne z/OS</b>	<b>z/OS oprávnění</b>
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

Tabulka 72. Příklad oprávnění k objektu tématu (pokračování)

Název tématu	Řetězec tématu	Oprávnění-ne z/OS	z/OS oprávnění
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, nadřazený uzel ve stromu určuje, zda má uživatel oprávnění přihlásit se k odběru na úrovni nadřazeného uzlu. Pokud ano, pak je přístup udělen. Není-li tomu tak, bude uvažovaný nadřazený uzel považován za nadřazený. 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` pokusí 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 nadřazenému 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`.

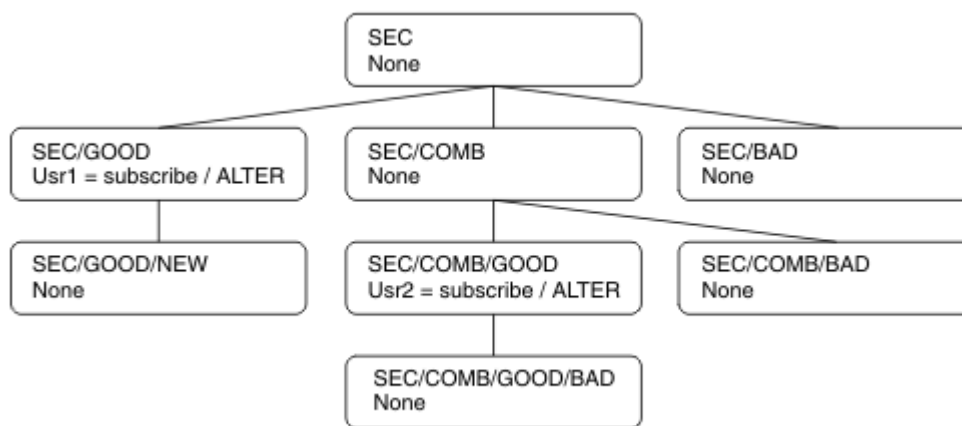
### Přihlášení k odběru pomocí řetězce tématu, ve kterém uzel tématu existuje

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 nadřazenému 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 nadřazeného 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 nadřazený 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 kdekoli 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 *not* 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 nadřazený uzel ve stromu považován za účelem určení, zda má uživatel oprávnění k uzavření odběru. Rekurze pokračuje, dokud není uděleno žádné oprávnění nebo je dosažen kořenový uzel.

## Definování, změna a odstranění odběru

Při vytvoření administrativně odběru se neprovádějí žádné kontroly zabezpečení odběru, místo použití požadavku rozhraní API produktu MQSUB . Administrátorovi bylo toto oprávnění uděleno prostřednictvím příkazu.

Jsou provedeny kontroly zabezpečení, aby bylo zajištěno, že publikování lze vložit do cílové fronty přidružené k odběru. Kontroly jsou prováděny stejným způsobem jako u požadavku MQSUB .

ID uživatele, které se používá pro tyto kontroly zabezpečení, závisí na vydávaný příkaz. Je-li zadán argument **SUBUSER** , ovlivní to způsob kontroly, jak ukazuje [Tabulka 73](#) na stránce 417:

<i>Tabulka 73. ID uživatele používaná pro kontroly zabezpečení pro příkazy</i>			
<b>Příkaz</b>	<b>SUBUSER zadán a prázdný</b>	<b>SUBUSER zadán a dokončen</b>	<b>SUBUSER není zadán</b>
	Použit ID administrátora		Použit ID uživatele z odběru LIKE
	Použit ID administrátora		Použijte ID.DEFAULT.SU uživateleB -je-li z SYSTEMprázdné, použijte ID administrátora.
	Použit ID administrátora		Použit 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.

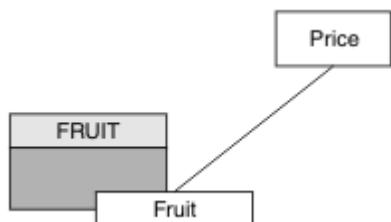
### Udělit uživateli přístup k odběru tématu

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 23. Příklad přístupu k objektu tématu

Tabulka 74. 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

- Zadejte příkaz MQSC DEF TOPIC(FRUIT) TOPICSTR('Price/Fruit').
- Udělte přístup následujícím způsobem:

- z/OS** z/OS :

Udělte přístup k produktu USER1 k odběru tématu "Price/Fruit" tím, že udělíte uživateli přístup k profilu produktu hlq.SUBSCRIBE.FRUIT. Toto provedte pomocí následujících příkazů obslužného programu RACF :

```
RDEFINE MXTOPIC hlq.SUBSCRIBE.FRUIT UACC(NONE)
PERMIT hlq.SUBSCRIBE.FRUIT CLASS(MXTOPIC) ID(USER1) ACCESS(ALTER)
```

- Ostatní platformy:

Udělte přístup k produktu USER1 k odběru tématu "Price/Fruit" tím, že udělíte uživateli přístup k objektu FRUIT. Provedte to pomocí příkazu autorizace pro platformu:

**Windows** **Linux** **UNIX** **Windows, systémy SYSTÉM UNIX a Linux**

```
setmqaut -t topic -n FRUIT -p USER1 +sub
```

**IBM i** **IBM i**

```
GRTMQAUT OBJ(FRUIT) OBJTYPE(*TOPIC) USER(USER1) AUT(*SUB)
```

## Výsledky

Když se produkt USER1 pokusí přihlásit k odběru tématu "Price/Fruit", výsledek je úspěšný.

Když se produkt USER2 pokusí přihlásit k odběru tématu "Price/Fruit", výsledkem je selhání zprávy MQRQ\_NOT\_AUTHORIZED spolu s:

- ▶ **z/OS** V systému z/OSse na konzole zobrazují následující zprávy, které zobrazují úplnou cestu zabezpečení prostřednictvím stromu témat, o který jste se pokusili:

```
ICH408I USER(USER2 ) ...
hlq.SUBSCRIBE.FRUIT ...

ICH408I USER(USER2 ) ...
hlq.SUBSCRIBE.SYSTEM.BASE.TOPIC ...
```

- ▶ **Windows** ▶ **Linux** ▶ **UNIX** Na ostatních platformách následující autorizační událost:

```
MQRQ_NOT_AUTHORIZED
ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
UserIdentifier       USER2
AdminTopicNames     FRUIT, SYSTEM.BASE.TOPIC
TopicString          "Price/Fruit"
```

- ▶ **IBM i** V systému IBMi následující autorizační událost:

```
MQRQ_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.

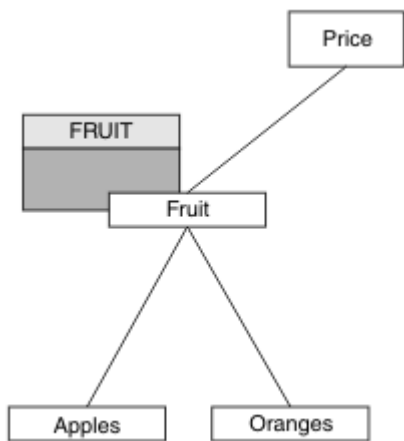
### Než začnete

Toto téma používá nastavení popsané v části [“Udělit uživateli přístup k odběru tématu”](#) na stránce 417.

### 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 nadřazený objekt administrativního tématu. Profil zabezpečení je zkontrolován na základě názvu daného objektu tématu.





Obrázek 24. Příklad udělení přístupu k tématu ve stromu témat

Tabulka 75. Požadavky na přístup pro ukázková témata a objekty témat

Téma	Je vyžadován přístup pro	Objekt tématu
Cena	Žádný uživatel	Není
Cena/Ovoce	USER1	OVOCE
Cena/Ovoce/ Jablka	USER1	
Cena/Ovoce/ Pomeranče	USER1	

V předchozí úloze USER1 byl udělen přístup k odběru tématu "Price/Fruit" udělením přístupu k profilu produktu hlq.SUBSCRIBE.FRUIT na serveru z/OS a k odběru přístupu k odběru profilu produktu FRUIT na jiných platformách. Tento jeden profil také uděluje přístup USER1 k odběru "Price/Fruit/Apples", "Price/Fruit/Oranges" a "Price/Fruit/#".

Když se produkt USER1 pokusí přihlásit k odběru tématu "Price/Fruit/Apples", výsledek je úspěšný.

Když se produkt USER2 pokusí přihlásit k odběru tématu "Price/Fruit/Apples", výsledkem je selhání zprávy MQRQ\_NOT\_AUTHORIZED spolu s:

- V systému z/OSse na konzole zobrazují následující zprávy, které zobrazují úplnou cestu zabezpečení prostřednictvím stromu témat, o který jste se pokusili:

```

ICH408I USER(USER2 ) ...
hlq.SUBSCRIBE.FRUIT ...

ICH408I USER(USER2 ) ...
hlq.SUBSCRIBE.SYSTEM.BASE.TOPIC ...
  
```

- Na ostatních platformách následující autorizační událost:

```

MQRQ_NOT_AUTHORIZED
ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
UserIdentifier       USER2
AdminTopicNames     FRUIT, SYSTEM.BASE.TOPIC
TopicString          "Price/Fruit/Apples"
  
```

Všimněte si následujícího:

- Zprávy, které obdržíte na z/OS, jsou totožné s těmi, které jste obdrželi v předchozí úloze, protože stejné objekty tématu a profily ovládají přístup.

- Zpráva události, kterou obdržíte na jiných platformách, je podobná té, která byla přijata v předchozí úloze, ale skutečný řetězec tématu se liší.

## Udělte jinému uživateli přístup k odběru pouze tématu hlouběji do stromu.

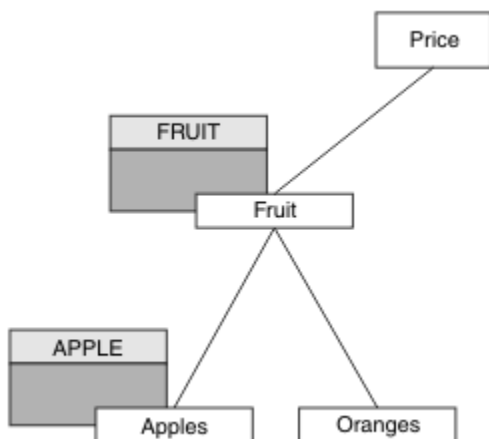
Toto téma je třetí ze seznamu úloh, které vám říkají, jak udělit přístup k odběru témat více než jedním uživatelem.

### Než začnete

Toto téma používá nastavení popsané v části [“Udělte uživateli přístup k odběru tématu hlouběji do stromu.”](#) na stránce 419.

### Informace o této úloze

V předchozí úloze byl USER2 odmítnut přístup k tématu "Price/Fruit/Apples". Toto téma informuje o tom, jak udělit přístup k tomuto tématu, ale ne k jiným tématům.



Obrázek 25. Udělení přístupu ke specifickým tématům v rámci stromu témat

Tabulka 76. Požadavky na přístup pro ukázková témata a objekty témat

Téma	Je vyžadován přístup pro	Objekt tématu
Cena	Žádný uživatel	Není
Cena/Ovoce	USER1	OVOCE
Cena/Ovoce/ Jablka	USER1 a USER2	Apple
Cena/Ovoce/ Pomeranče	USER1	

Definujte nový objekt tématu následujícím způsobem:

### Postup

1. Zadejte příkaz `MQSC DEF TOPIC(APPLE) TOPICSTR('Price/Fruit/Apples')`.
2. Udělte přístup následujícím způsobem:

-  **z/OS** :

V předchozí úloze USER1 byl udělen přístup k odběru tématu "Price/Fruit/Apples" udělením přístupu uživatele k profilu produktu `hlq.SUBSCRIBE.FRUIT`.

Tento jediný profil také udělil USER1 přístup k odběru "Price/Fruit/Oranges" "Price/Fruit/#" a tento přístup zůstává i s přidáním nového objektu tématu a s přidruženými profily.

Udělte přístup k produktu USER2 k odběru tématu "Price/Fruit/Apples" tím, že udělíte uživateli přístup k profilu produktu hlq.SUBSCRIBE.APPLE. Toto proveďte pomocí následujících příkazů obslužného programu RACF :

```
RDEFINE MXTOPIC hlq.SUBSCRIBE.APPLE UACC(NONE)
PERMIT hlq.SUBSCRIBE.FRUIT APPLE(MXTOPIC) ID(USER2) ACCESS(ALTER)
```

- Ostatní platformy:

V předchozí úloze USER1 byl udělen přístup k odběru tématu "Price/Fruit/Apples" tím, že uživateli udělil přístup k odběru profilu FRUIT.

Tento jediný profil také udělil USER1 přístup k odběru "Price/Fruit/Oranges" a "Price/Fruit/#" a tento přístup zůstává dokonce i s přidáním nového objektu tématu a s tím, že k němu jsou přidruženy profily.

Udělte přístup k produktu USER2 k přihlášení k odběru tématu "Price/Fruit/Apples" tím, že uživateli přidělíte přístup k odběru pro profil produktu APPLE. Proveďte to pomocí příkazu autorizace pro platformu:

**Windows** **Linux** **UNIX** **Windows, systémy SYSTÉM UNIX a Linux**

```
setmqaut -t topic -n APPLE -p USER2 +sub
```

**IBM i** **IBM i**

```
GRTMQAUT OBJ(APPLE) OBJTYPE(*TOPIC) USER(USER2) AUT(*SUB)
```

## Výsledky

Pokud se v produktu z/OS při pokusu USER1 o přihlášení k odběru tématu "Price/Fruit/Apples" nezdaří první kontrola zabezpečení v profilu produktu hlq.SUBSCRIBE.APPLE, ale při přesunu stromu profilu produktu hlq.SUBSCRIBE.FRUIT umožňuje přihlášení k odběru USER1, odběr je úspěšný a pro volání MQSUB se neodešle žádný návratový kód. Zpráva RACF ICH se však vygeneruje pro první kontrolu:

```
ICH408I USER(USER1 ) ...
hlq.SUBSCRIBE.APPLE ...
```

Když se produkt USER2 pokusí přihlásit k odběru tématu "Price/Fruit/Apples", výsledek je úspěšný, protože kontrola zabezpečení proběhne na prvním profilu.

Když se produkt USER2 pokusí přihlásit k odběru tématu "Price/Fruit/Oranges", výsledkem je selhání zprávy MQRC\_NOT\_AUTHORIZED spolu s:

- **z/OS** V systému z/OS se 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 ...
```

- **Windows** **Linux** **UNIX** Na platformách Windows, SYSTÉM UNIX a Linux , následující autorizační událost:

```

MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRC_SUB_NOT_AUTHORIZED
UserIdentifier       USER2
AdminTopicNames     FRUIT, SYSTEM.BASE.TOPIC
TopicString          "Price/Fruit/Oranges"

```

- **IBM i** V systému IBMi následující autorizační událost:

```

MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRC_SUB_NOT_AUTHORIZED
UserIdentifier       USER2
AdminTopicNames     FRUIT, SYSTEM.BASE.TOPIC
TopicString          "Price/Fruit/Oranges"

```

Nevýhodou tohoto nastavení je to, že v systému z/OSobdržíte na konzole další zprávy produktu ICH . Tomuto se můžete vyhnout, pokud jste strom témat zabezpečili jiným způsobem.

## Změnit řízení přístupu tak, aby se předešlo dalším zprávám

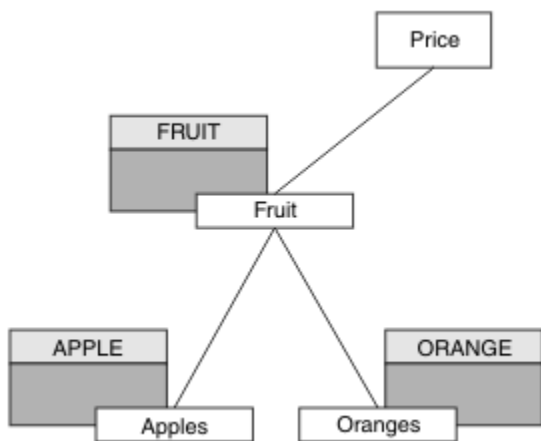
Toto téma je čtvrté v seznamu úloh, které vám sdělují, jak udělit přístup k odběru témat více uživateli a vyhnout se dalším zprávám RACF ICH408I na serveru z/OS.

### Než začnete

Toto téma vylepšuje nastavení popsané v tématu “[Udělte jinému uživateli přístup k odběru pouze tématu hlouběji do stromu.](#)” na stránce 421 , takže se vyhnete dalším chybovým zprávám.

### Informace o této úloze

Toto téma vám říká, jak udělit přístup k tématům hlouběji ve stromu a jak odstranit přístup k tématu níže ve stromu, když jej žádný uživatel nepotřebuje.



Obrázek 26. Příklad udělení řízení přístupu pro zamezení dalších zpráv.

Definujte nový objekt tématu následujícím způsobem:

### Postup

1. Zadejte příkaz `MQSC DEF TOPIC(ORANGE) TOPICSTR('Price/Fruit/Oranges')`.
2. Udělte přístup následujícím způsobem:

- **z/OS** **z/OS** :

Definujte nový profil a přidejte k tomuto profilu přístup a existující profily. Toto proveďte pomocí následujících příkazů obslužného programu RACF :

```
RDEFINE MXTOPIC hlq.SUBSCRIBE.ORANGE UACC(NONE)
PERMIT hlq.SUBSCRIBE.ORANGE CLASS(MXTOPIC) ID(USER1) ACCESS(ALTER)
PERMIT hlq.SUBSCRIBE.APPLE CLASS(MXTOPIC) ID(USER1) ACCESS(ALTER)
```

- Ostatní platformy:

Nastavení ekvivalentního přístupu pomocí příkazů autorizace pro platformu:

**Windows** **Linux** **UNIX** **Windows, systémy SYSTÉM UNIX a Linux**

```
setmqaut -t topic -n ORANGE -p USER1 +sub
setmqaut -t topic -n APPLE -p USER1 +sub
```

**IBM i** **IBM i**

```
GRTMQAUT OBJ(ORANGE) OBJTYPE(*TOPIC) USER(USER1) AUT(*SUB)
GRTMQAUT OBJ(APPLE) OBJTYPE(*TOPIC) USER(USER1) AUT(*SUB)
```

## Výsledky

Pokud se v produktu z/OS pokusí produkt USER1 přihlásit k odběru tématu "Price/Fruit/Apples" , je první kontrola zabezpečení profilu hlq.SUBSCRIBE . APPLE úspěšná.

Podobně platí, že když se produkt USER2 pokusí přihlásit k odběru tématu "Price/Fruit/Apples" , výsledek je úspěšný, protože kontrola zabezpečení proběhne na prvním profilu.

Když se produkt USER2 pokusí přihlásit k odběru tématu "Price/Fruit/Oranges" , výsledkem je selhání zprávy MQRQ\_NOT\_AUTHORIZED spolu s:

- **z/OS** V systému z/OSse na konzole zobrazují následující zprávy, které zobrazují úplnou cestu zabezpečení prostřednictvím stromu témat, o který jste se pokusili:

```
ICH408I USER(USER2 ) ...
hlq.SUBSCRIBE.ORANGE ...

ICH408I USER(USER2 ) ...
hlq.SUBSCRIBE.FRUIT ...

ICH408I USER(USER2 ) ...
hlq.SUBSCRIBE.SYSTEM.BASE.TOPIC ...
```

- **Windows** **Linux** **UNIX** Na ostatních platformách následující autorizační událost:

```
MQRQ_NOT_AUTHORIZED
ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
UserIdentifier       USER2
AdminTopicNames     ORANGE, FRUIT, SYSTEM.BASE.TOPIC
TopicString          "Price/Fruit/Oranges"
```

- **IBM i** V systému IBMi následující autorizační událost:

```
MQRQ_NOT_AUTHORIZED
ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
UserIdentifier       USER2
AdminTopicNames     ORANGE, FRUIT, SYSTEM.BASE.TOPIC
TopicString          "Price/Fruit/Oranges"
```

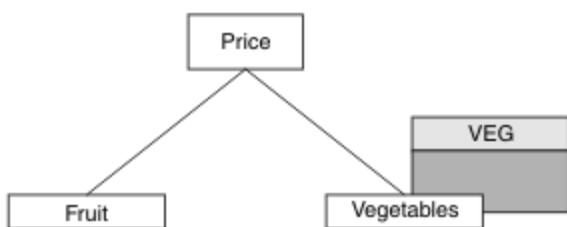
## Udělit přístup uživateli k publikování v rámci tématu

Toto téma je první v seznamu úloh, které vám říká, jak udělit přístup k publikačním tématům více než jednoho uživatele.

### Informace o této úloze

Tato úloha předpokládá, že na pravé straně stromu témat neexistují žádné objekty administrativních témat, ani nejsou definovány žádné profily pro publikování. Předpokládá se, že vydavatelé používají pouze řetězec tématu.

Aplikace může publikovat do tématu poskytnutím objektu tématu nebo řetězce tématu nebo kombinací obou těchto témat. Bez ohledu na způsob, jakým aplikace vybere aplikace, bude tento efekt ve stromu témat publikován v určitém bodě. Je-li tento bod ve stromu témat reprezentován objektem administrativního tématu, je profil zabezpečení zkontrolován na základě názvu daného objektu tématu. Příklad:



Obrázek 27. Udělení přístupu pro publikování k tématu

Tabulka 77. 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

- Zadejte příkaz `MQSC DEF TOPIC(VEG) TOPICSTR('Price/Vegetables')`.
- Udělte přístup následujícím způsobem:

-  **z/OS :**

Udělte přístup k produktu USER1 k publikování v rámci tématu "Price/Vegetables" udělením přístupu uživatele k profilu produktu `hlq.PUBLISH.VEG`. Toto provedte pomocí následujících příkazů obslužného programu RACF :

```
RDEFINE MXTOPIC hlq.PUBLISH.VEG UACC(NONE)
PERMIT hlq.PUBLISH.VEG CLASS(MXTOPIC) ID(USER1) ACCESS(UPDATE)
```

- Ostatní platformy:

Udělte přístup k produktu USER1 k publikování v rámci tématu "Price/Vegetables" udělením přístupu uživatele k profilu produktu VEG. Proveďte to pomocí příkazu autorizace pro platformu:

   **Windows, systémy SYSTÉM UNIX a Linux**

```
setmqaut -t topic -n VEG -p USER1 +pub
```

```
GRTMQAUT OBJ(VEG) OBJTYPE(*TOPIC) USER(USER1) AUT(*PUB)
```

## Výsledky

Když se produkt USER1 pokusí o publikování do tématu "Price/Vegetables", výsledek je úspěšný; to znamená, že volání MQOPEN je úspěšné.

Když se příkaz USER2 pokusí publikovat do tématu "Price/Vegetables", volání MQOPEN selže se zprávou MQRC\_NOT\_AUTHORIZED, spolu s:

- z/OS V systému z/OSse na konzole zobrazují následující zprávy, které zobrazují úplnou cestu zabezpečení prostřednictvím stromu témat, o který jste se pokusili:

```

ICH408I USER(USER2  ) ...
hlq.PUBLISH.VEG ...

ICH408I USER(USER2  ) ...
hlq.PUBLISH.SYSTEM.BASE.TOPIC ...
    
```

- Windows Linux UNIX Na ostatních platformách následující autorizační událost:

```

MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRC_OPEN_NOT_AUTHORIZED
UserIdentifier       USER2
AdminTopicNames     VEG, SYSTEM.BASE.TOPIC
TopicString          "Price/Vegetables"
    
```

- IBM i V systému IBMi následující autorizační událost:

```

MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRC_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.

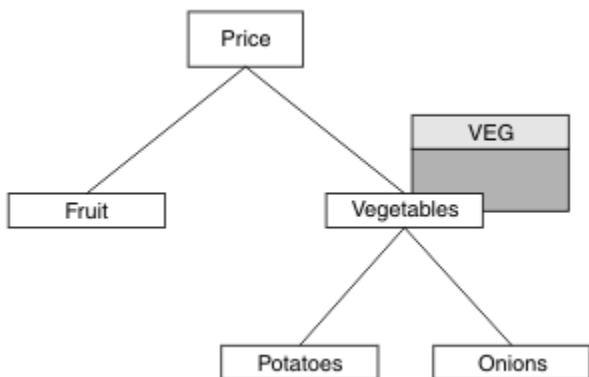
Toto téma je druhé v seznamu úloh, které vás informují o tom, jak udělit přístup k publikačním tématům více uživateli než jednomu uživateli.

### Než začnete

Toto téma používá nastavení popsané v části [“Udělit přístup uživateli k publikování v rámci tématu”](#) na stránce 425.

### Informace o této úloze

Pokud bod ve stromu témat obsahující publikování aplikace není reprezentován administrativním objektem tématu, přesuňte strom tak, aby byl umístěn nejbližší nadřazený objekt administrativního tématu. Profil zabezpečení je zkontrolován na základě názvu daného objektu tématu.



Obrázek 28. Udělení přístupu pro publikování k tématu v rámci stromu témat

Tabulka 78. 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 veřejnému tématu "Price/Vegetables/Potatoes" tím, že mu udělíte přístup k profilu produktu hlq.PUBLISH.VEG na serveru z/OS nebo publikoval přístup k profilu produktu VEG na jiných platformách. Tento jeden profil také uděluje přístup USER1 k publikaci v "Price/Vegetables/Onions".

Když se USER1 pokusí publikovat v tématu "Price/Vegetables/Potatoes", výsledek je úspěšný; to je volání MQOPEN je úspěšné.

Když se produkt USER2 pokusí přihlásit k odběru tématu "Price/Vegetables/Potatoes", výsledek se nezdařil; volání MQOPEN se nezdaří se zprávou MQRC\_NOT\_AUTHORIZED, spolu s:

- V systému z/OSse na konzole zobrazují následující zprávy, které zobrazují úplnou cestu zabezpečení prostřednictvím stromu témat, o který jste se pokusili:

```

ICH408I USER(USER2 ) ...
hlq.PUBLISH.VEG ...

ICH408I USER(USER2 ) ...
hlq.PUBLISH.SYSTEM.BASE.TOPIC ...
  
```

- Na ostatních platformách následující autorizační událost:

```

MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRC_OPEN_NOT_AUTHORIZED
UserIdentifier       USER2
AdminTopicNames     VEG, SYSTEM.BASE.TOPIC
TopicString          "Price/Vegetables/Potatoes"
  
```

Všimněte si následujícího:

- Zprávy, které obdržíte na z/OS, jsou totožné s těmi, které jste obdrželi v předchozí úloze, protože stejné objekty tématu a profily ovládají přístup.



- Zpráva události, kterou obdržíte na jiných platformách, je podobná té, která byla přijata v předchozí úloze, ale skutečný řetězec tématu se liší.

## Udělit přístup pro publikování a odběr

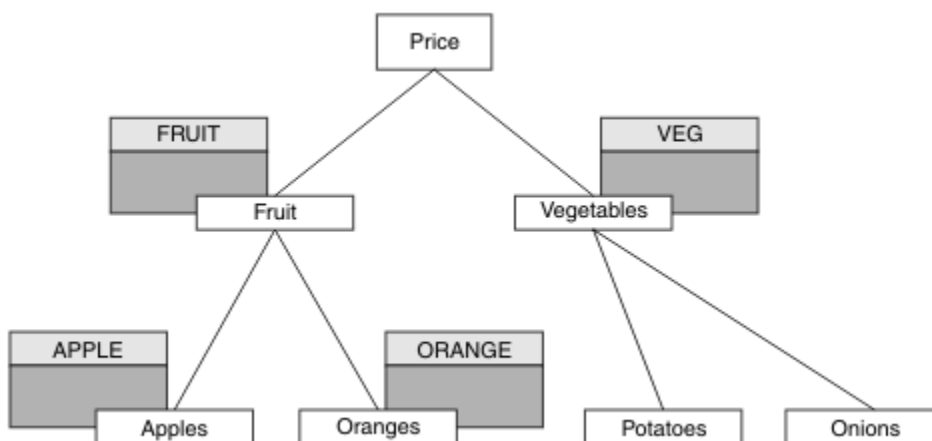
Toto téma je poslední v seznamu úloh, které vás informují o tom, jak udělit přístup k publikování a k odběru témat více než jedním uživatelem.

### Než začnete

Toto téma používá nastavení popsané v části [“Udělte uživateli přístup k tématu hlouběji do stromu.”](#) na stránce 426.

### Informace o této úloze

V předchozí úloze USER1 byl poskytnut přístup k odběru tématu "Price/Fruit". Toto téma vám sděluje, jak udělit přístup tomuto uživateli k publikování v tomto tématu.



Obrázek 29. Udělení přístupu pro publikování a odběr

Tabulka 79. Příklad požadavků na publikování a přihlášení k odběru

Téma	Je vyžadován přístup pro	Požadovaný přístup pro publikování	Objekt tématu
Cena	Žádný uživatel	Žádný uživatel	Není
Cena/Ovoce	USER1	USER1	OVOCE
Cena/Ovoce/Jablka	USER1 a USER2		Apple
Cena/Ovoce/Pomeranče	USER1		ORANŽOVÁ

### Postup

Udělte přístup následujícím způsobem:

-  **z/OS** :

V dřívější úloze USER1 byl udělen přístup k odběru tématu "Price/Fruit" udělením přístupu uživatele k profilu produktu hlq.SUBSCRIBE.FRUIT.

Chcete-li publikovat na téma "Price/Fruit" , udělte přístup k USER1 profilu hlq.PUBLISH.FRUIT . Toto proveďte pomocí následujících příkazů obslužného programu RACF :

```
RDEFINE MXTOPIC hlq.PUBLISH.FRUIT UACC(NONE)
PERMIT hlq.PUBLISH.FRUIT CLASS(MXTOPIC) ID(USER1) ACCESS(ALTER)
```

- Ostatní platformy:

Udělte přístup k produktu USER1 k publikování na téma "Price/Fruit" tím, že uživateli udělíte přístup pro publikování k profilu produktu FRUIT . Proveďte to pomocí příkazu autorizace pro platformu:

**Windows** **Linux** **UNIX** **Windows, systémy SYSTÉM UNIX a Linux**

```
setmqaut -t topic -n FRUIT -p USER1 +pub
```

**IBM i** **IBM i**

```
GRTMQAUT OBJ(FRUIT) OBJTYPE(*TOPIC) USER(USER1) AUT(*PUB)
```

## Výsledky

On z/OS, when USER1 attempts to publish to topic "Price/Fruit" the security check on the MQOPEN call passes.

Když se příkaz USER2 pokusí o publikaci na téma "Price/Fruit" , výsledkem je selhání se zprávou MQRC\_NOT\_AUTHORIZED společně s:

- **z/OS** V systému z/OSse na konzole zobrazují následující zprávy, které zobrazují úplnou cestu zabezpečení prostřednictvím stromu témat, o který jste se pokusili:

```
ICH408I USER(USER2 ) ...
hlq.PUBLISH.FRUIT ...

ICH408I USER(USER2 ) ...
hlq.PUBLISH.SYSTEM.BASE.TOPIC ...
```

- **Windows** **Linux** **UNIX** Na platformách Windows, UNIXa Linux následující autorizační událost:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRC_OPEN_NOT_AUTHORIZED
UserIdentifier       USER2
AdminTopicNames     FRUIT, SYSTEM.BASE.TOPIC
TopicString          "Price/Fruit"
```

- **IBM i** V systému IBMi následující autorizační událost:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRC_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 80. Úplný seznam přístupových oprávnění vedoucích k příkladům zabezpečení

Téma	Je vyžadován přístup pro	Požadovaný přístup pro publikování	Objekt tématu
Cena	Žádný uživatel	Žádný uživatel	Není
Cena/Ovoce	USER1	USER1	OVOCE
Cena/Ovoce/ Jablka	USER1 a USER2		Apple
Cena/Ovoce/ Pomeranče	USER1		ORANŽOVÁ
Cena/ Zelenina		USER1	VEG.
Cena/ Zelenina/ Potatony			
Cena/ Zelenina/ Onivy			

Pokud máte různé požadavky pro zabezpečení přístupu na různých úrovních ve stromu témat, pečlivě plánování zajišťuje, že v protokolu konzoly produktu z/OS nebude docházet k nadbytečným varováním zabezpečení. Nastavení zabezpečení na správné úrovni v rámci stromu se vyhýbá zavádějícím zprávám zabezpečení.

## Zabezpečení odběru

### OPRÁVNĚNÍ UŽIVATELE MQSO\_ALTERNATE\_USER\_AUTHORITY

Pole ID AlternateUserobsahuje identifikátor uživatele, který se má použít k ověření tohoto volání MQSUB. Volání může být úspěšné pouze v případě, že je tento identifikátor AlternateUserautorizován k přihlášení k odběru tématu s určenými volbami přístupu bez ohledu na to, zda je identifikátor uživatele, pod kterým je aplikace spuštěna, oprávněn tak učinit.

### KONTEXT MQSO\_SET\_IDENTITY\_CONTEXT

Cílem odběru je použít data evidence a údaje o identitě aplikace zadané v polích PubAccountinga PubApplIdentityData .

Je-li tato volba zadána, provede se stejná kontrola autorizace jako v případě, že k cílové frontě bylo přístupováno 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 přidruжены výchozí informace o kontextu:

Tabulka 81. 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.

<i>Tabulka 81. Výchozí informace o kontextu publikování (pokračování)</i>	
<b>Pole v MQMD</b>	<b>Použitá hodnota</b>
<i>AccountingToken</i>	Je-li to možné, určeno z prostředí; v opačném případě nastavte hodnotu MQACT_NONE.
<i>ApplIdentityData</i>	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 pozměnění odběru (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. Vlastníci ID uživatele odběru lze zobrazit pomocí příkazu DISPLAY SBSTATUS.

Není-li zadán parametr MQSO\_ANY\_USERID nebo MQSO\_FIXED\_USERID, je výchozí hodnota MQSO\_FIXED\_USERID.

## Zabezpečení publikování/odběru mezi správci front

Interní zprávy publikování/odběru, jako jsou například proxy odběry a publikace, jsou vloženy do systémových front publikování/odběru s použitím běžných pravidel zabezpečení kanálu. Informace a diagramy v tomto tématu zdůrazňují různé procesy a ID uživatelů, které se podílejí na doručování těchto zpráv.

### Lokální řízení přístupu

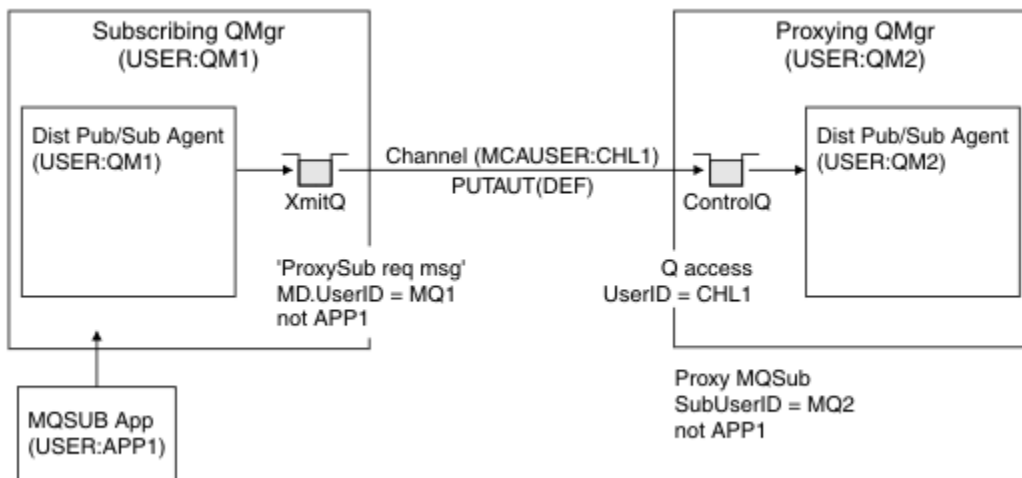
Přístup k tématům pro publikování a odběry je řízen lokálními definicemi zabezpečení a pravidly, které jsou popsány v tématu [Zabezpečení publikování/odběru](#). V systému z/OS není k zavedení řízení přístupu požadován žádný lokální objekt tématu. Pro řízení přístupu na jiných platformách není vyžadováno žádné lokální téma. Administrátoři se mohou rozhodnout použít řízení přístupu k objektům klastrovaných témat bez ohledu na to, zda již v klastru existují.

Systémoví administrátoři jsou odpovědní za řízení přístupu na svém lokálním systému. Musí důvěřovat administrátorům ostatních členů hierarchie nebo kolektivitu klastru, aby byli odpovědní za jejich zásadu řízení přístupu. Vzhledem k tomu, že řízení přístupu je definováno pro každý samostatný počítač, je pravděpodobné, že bude tíživé, je-li zapotřebí kontrola na úrovni pokuty. Ve stromu témat nemusí být nutné definovat žádné řízení přístupu nebo řízení přístupu k vyšším objektům. Řízení přístupu na úrovni FGT lze definovat pro každou dílčí divizi oboru názvů témat.

### Vytvoření proxy odběru

Důvěryhodnost organizace pro připojení správce front k vašemu správci front je potvrzena běžnými prostředky ověřování kanálu. Je-li tato důvěryhodná organizace také povolena k distribuovanému publikování/odběru, provede se kontrola oprávnění. Kontrola se provede, když kanál vloží zprávu do fronty distribuovaných publikování/odběru. Je-li například vložena zpráva do fronty SYSTEM . INTER . QMGR . CONTROL . ID uživatele pro kontrolu oprávnění fronty závisí na hodnotách typu PUTAUT přijímajícího kanálu. Příklad: ID uživatele kanálu, MCAUSER, kontext zprávy, v závislosti na hodnotě a platformě. Další informace o zabezpečení kanálu naleznete v tématu [Zabezpečení kanálů](#).

Odběry proxy se provádějí s ID uživatele distribuovaného agenta publikování/odběru ve vzdáleném správci front. Například QM2 v [Obrázek 30](#) na stránce 432. Uživateli je poté snadno udělen přístup k lokálním profilům objektů tématu, protože ID uživatele je v systému definováno a neexistují tedy žádné konflikty domén.



Obrázek 30. Zabezpečení odběru proxy, provedení odběru

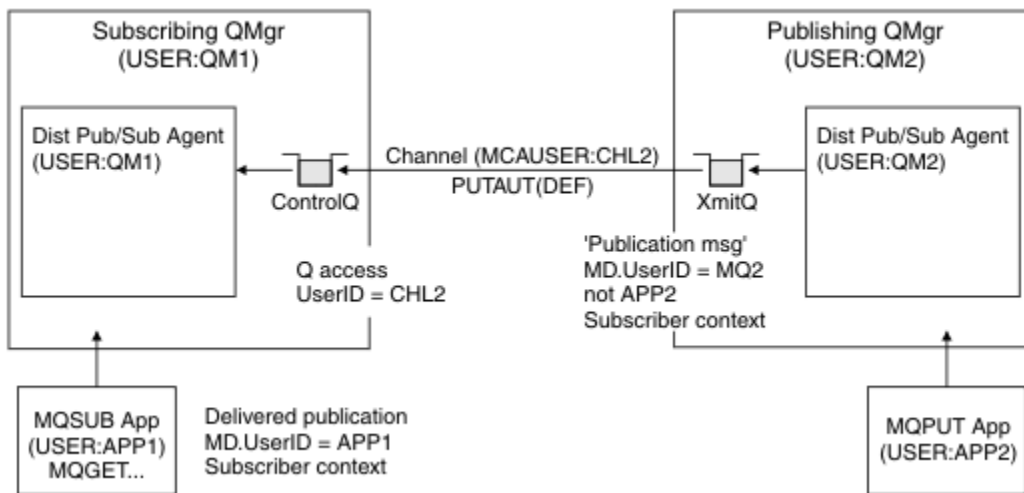
### Odeslání vzdálených publikování

Je-li publikace vytvořena ve správci front publikování, je vytvořena kopie publikování pro každý odběr proxy. Kontext zkopírované publikace obsahuje kontext ID uživatele, který vytvořil odběr; QM2 v produktu

Obrázek 31 na stránce 433. Proxy odběr se vytvoří s cílovou frontou, která je vzdálenou frontou, takže je zpráva publikování vyřešena do přenosové fronty.

Důvěryhodnost organizace pro připojení svého správce front QM2k jinému správci front QM1 je potvrzena normálním ověřováním kanálu. Je-li tato důvěryhodná organizace poté povolena pro distribuované publikování/odběr, provede se kontrola oprávnění, když kanál vloží zprávu publikování do fronty publikování distribuovaného publikování/odběru SYSTEM . INTER . QMGR . PUBS. ID uživatele pro kontrolu oprávnění fronty závisí na hodnotě parametru PUTAUT přijímajícího kanálu (například ID uživatele kanálu, MCAUSER, kontext zprávy a další informace v závislosti na hodnotě a platformě). Další informace o zabezpečení kanálu naleznete v tématu Zabezpečení kanálů.

Když se zpráva o publikování dostane do správce front odběru, provede se další příkaz MQPUT pro dané téma pod oprávněním správce front a kontext s touto zprávou je nahrazen kontextem každého z lokálních odběratelů, protože každá z nich má danou zprávu.



Obrázek 31. Zabezpečení odběru proxy, postoupení publikací

V systému, kde bylo zvažováno, že se týká zabezpečení, je pravděpodobné, že procesy distribuovaného publikování/odběru budou spuštěny pod ID uživatele ve skupině mqm , parametr MCAUSER na kanálu je prázdný (předvolba) a zprávy se doručí do různých systémových front podle potřeby. Nezabezpečený systém umožňuje snadné nastavení koncepce k demonstraci distribuovaného publikování/odběru.

V systému, kde je zabezpečení vážnější, se na tyto interní zprávy vztahují stejné ovládací prvky zabezpečení jako každá zpráva, která se přešla přes kanál.

Pokud je kanál nastaven s neprázdnou hodnotou MCAUSER a hodnotou PUTAUT určující, že MCAUSER musí být zkontrolována, pak musí mít MCAUSER udělen přístup k frontám SYSTEM . INTER . QMGR . \* . Existuje-li více různých vzdálených správců front s kanály spuštěnými pod různými identifikátory MCAUSER , je třeba všem těmto ID uživatelů udělit přístup k frontám produktu SYSTEM . INTER . QMGR . \* . Kanály spuštěné pod různými ID MCAUSER se mohou vyskytnout například v případě, že je v jednom správci front nakonfigurováno více hierarchických připojení.

Je-li kanál nastaven s hodnotou PUTAUT určující, že je použit kontext zprávy, pak je přístup k frontám SYSTEM . INTER . QMGR . \* kontrolován na základě ID uživatele uvnitř interní zprávy. Protože všechny tyto zprávy jsou vloženy s ID uživatele distribuovaného agenta publikování/odběru ze správce front, který odesílá interní zprávu, nebo zprávu publikování (viz Obrázek 31 na stránce 433 ), není příliš velká sada ID uživatelů pro udělení přístupu k různým systémovým frontám (jeden pro vzdáleného správce front), pokud chcete tímto způsobem nastavit zabezpečení distribuovaného publikování/odběru. Stále má všechny stejné problémy, které zabezpečení kontextu kanálu vždy má, a to z různých domén ID uživatele a skutečnost, že ID uživatele ve zprávě nemusí být definováno v přijímajícím systému. Je to však naprosto přijatelný způsob, jak se v případě potřeby spustit.

**z/OS** Zabezpečení systémové fronty poskytuje seznam front a přístup, který je zapotřebí k bezpečnému nastavení distribuovaného prostředí publikování/odběr. Pokud dojde k selhání interních

zpráv nebo publikování kvůli narušení zabezpečení, kanál zapíše zprávu do protokolu normálním způsobem a zprávy lze odeslat do fronty nedoručených zpráv v souladu s normálním zpracováním chyb kanálu.

Všechny systémy zpráv mezi správci front pro účely distribuovaných publikování/odběru se spouštějí s použitím běžného zabezpečení kanálu.

Informace o omezení publikování a odběrů proxy na úrovni tématu naleznete v tématu [Zabezpečení publikování/odběru](#).

## Použití výchozích ID uživatelů s hierarchií správce front

Pokud máte hierarchii správců front spuštěných na různých platformách a používáte výchozí ID uživatelů, všimněte si, že tato výchozí ID uživatele se liší mezi platformami a nemusí být známá na cílové platformě. Výsledkem je, že správce front spuštěný na jedné platformě zamítá zprávy přijaté od správců front na jiných platformách s kódem příčiny MQRC\_NOT\_AUTHORIZED.

Chcete-li zabránit odmítnutí zpráv, je třeba přidat k výchozím ID uživatele, která se používají na jiných platformách, následující oprávnění:

- \*PUT \*GET oprávnění na SYSTEM.BROKER. fronty
- \*PUB \*SUB oprávnění na systému SYSTEM.BROKER. Témata
- \*ADMCR \*ADMDEL \*ADMCHG oprávnění na SYSTEM.BROKER.CONTROL.QUEUE fronta.

Výchozí jména uživatelů s hierarchií správce front jsou následující:

Platforma	Předvolené ID uživatele
Windows	MUSR_MQADMIN
Systémy SYSTÉM UNIX a Linux	mqm
IBM i	QMQM
z/OS	ID uživatele adresního prostoru inicializátoru kanálu

Vytvořte a udělte přístup k ID uživatele 'qmqm', je-li hierarchicky připojen ke správci front v produktu IBM i for Queue Managers v platformách Windows, UNIX, Linux a z/OS .

Vytvořte a udělte přístup k ID uživatele 'mqm', je-li hierarchicky připojen ke správci front v systémech Windows, UNIX nebo Linux pro správce front na platformách IBM i a z/OS .

Vytvořte a udělte uživatelský přístup k ID uživatele adresního prostoru iniciátoru kanálu produktu z/OS , pokud je hierarchicky připojen ke správci front v produktu z/OS for Queue Managers v platformách Windows, UNIX, Linux a IBM i .

ID uživatelů mohou rozlišovat malá a velká písmena. Původní správce front (pokud systémy IBM i, Windows, UNIX nebo Linux ) vynutí, aby ID uživatele bylo vše velkými písmeny. Přijímající správce front (pokud systémy Windows, UNIX nebo Linux ) vynutí, aby ID uživatele bylo zadáno malými písmeny. Proto musí být všechna ID uživatelů vytvořená na systémech SYSTÉM UNIX a Linux vytvořena ve svém formátu s malými písmeny. Byla-li instalována uživatelská procedura pro zprávy, vynucuje se ID uživatele velkými nebo malými písmeny. Je třeba věnovat pozornost tomu, jak procedura ukončení zprávy zpracovává ID uživatele.

Chcete-li se vyhnout potenciálním problémům s převodem ID uživatelů, postupujte takto:

- V systémech UNIX, Linux a Windows se ujistěte, že ID uživatelů jsou uvedena malými písmeny.
- V systémech IBM i a z/OS kontrolujte, zda jsou ID uživatelů zadána velkými písmeny.

Pokud používáte ověření jména uživatele a hesla pro připojení ke správci databází, můžete je uložit do úložiště pověření XA produktu MQ, abyste se vyhnuli ukládání hesla do prostého textu v souboru `qm.ini`.

### Aktualizujte XAOpenString pro správce prostředků

Chcete-li použít úložiště pověření, musíte upravit XAOpenString v souboru `qm.ini`. Řetězec se používá pro připojení ke správci databází. Do pole XAOpenString můžete určit, kde se má nahradit jméno uživatele a heslo, určete výměnná pole.

- Pole `+USER+` se nahradí hodnotou jména uživatele uloženou v úložišti XACredentials.
- Pole `+PASSWORD+` je nahrazeno hodnotou hesla uloženou v úložišti XACredentials.

Následující příklady ukazují, jak upravit XAOpenString tak, aby používal soubor pověření pro připojení k databázi.

#### Připojení k databázi Db2

```
XAResourceManager:  
Name=mydb2  
SwitchFile=db2swit  
XAOpenString=db=mydbname,uid=+USER+,pwd=+PASSWORD+,toc=t  
ThreadOfControl=THREAD
```

#### Připojení k databázi Oracle

```
XAResourceManager:  
Name=myoracle  
SwitchFile=oraswit  
XAOpenString=Oracle_XA+Acc=P/+USER+/+PASSWORD++SesTm=35  
+LogDir=/tmp+threads=true  
ThreadOfControl=THREAD
```

### Práce s pověřením pro databázi do úložiště pověření XA produktu MQ

Poté, co aktualizujete soubor `qm.ini` s nahraditelnými řetězci pověření, musíte přidat jméno uživatele a heslo do úložiště pověření MQ pomocí příkazu `setmqxacred`. `setmqxacred` můžete také použít k úpravě existujících pověření, odstranění pověření nebo seznamu pověření. Následující příklady uvádějí některé typické případy použití:

#### Přidání pověření

Následující příkaz bezpečně uloží jméno uživatele a heslo pro správce front QM1 pro prostředek `mqdb2`.

```
setmqxacred -m QM1 -x mydb2 -u user1 -p Password2
```

#### Aktualizace pověření

Chcete-li aktualizovat jméno uživatele a heslo použité pro připojení k databázi, znovu zadejte příkaz `setmqxacred` s novým uživatelským jménem a heslem:

```
setmqxacred -m QM1 -x mydb2 -u user3 -p Password4
```

Aby se změny projevíly, je třeba restartovat správce front.

#### Odstranění pověření

Následující příkaz odstraní pověření:



```
setmqxacred -m QM1 -x mydb2 -d
```

### Výpis pověření

Následující příkaz vypíše seznam pověření:

```
setmqxacred -m QM1 -l
```

### Související informace

#### setmqxacred

Windows

Linux

UNIX

## Zabezpečení klientů AMQP

Zabezpečte připojení klientů AMQP pomocí řady mechanismů zabezpečení a zajistěte, aby byla data vhodně chráněna v síti. Můžete sestavit zabezpečení do aplikací MQ Light . Můžete také použít existující funkce zabezpečení produktu IBM MQ s klienty AMQP stejným způsobem, jako jsou funkce použity pro jiné aplikace.

### Pravidla ověření kanálu (CHLAUTH)

Můžete použít pravidla ověření kanálu k omezení připojení TCP ke správci front. Kanály AMQP podporují použití pravidel pro ověřování kanálu, které jste nakonfigurovali pro správce front. Jsou-li pravidla ověřování kanálu definována s profilem, který odpovídá libovolnému kanálu AMQP ve správci front, budou tato pravidla použita pro tyto kanály. Při výchozím nastavení je v nových správcích front produktu IBM MQ povoleno ověřování kanálu, takže je třeba před použitím kanálu AMQP dokončit alespoň nějakou konfiguraci.

Další informace o tom, jak konfigurovat pravidla ověřování kanálu pro povolení připojení AMQP k vašemu správci front, najdete v tématu [Vytvoření a použití kanálů AMQP](#).

### Ověření připojení (CONNAUTH)

V 8.0.0.4

Pro ověření připojení ke správci front můžete použít ověření připojení. Kanály AMQP podporují použití ověření připojení pro řízení přístupu ke správci front z aplikací AMQP.

Protokol AMQP používá rámec SASL (Simple Authentication and Security Layer) k určení, jak je připojení ověřováno. K dispozici jsou různé mechanismy SASL a IBM MQ podporuje dva mechanismy SASL: ANONYMOUS a PLAIN.

V případě ANONYMOUS nebyla z klienta do správce front pro ověření předávána žádná pověření. Pokud má objekt MQ AUTHINFO uvedený v atributu CONNAUTH hodnotu CHCKCLNT nebo REQDADM (pokud se připojuje jako administrativní uživatel), připojení se odmítne. Je-li hodnota CHCKCLNT NONE nebo OPTIONAL, připojení je akceptováno.

V případě služby PLAIN je pro ověření předáno jméno uživatele a heslo z klienta do správce front. Pokud má objekt MQ AUTHINFO uvedený v atributu CONNAUTH hodnotu CHCKCLNT, je hodnota NONE, připojení odmítnuto. Je-li hodnota parametru CHCKCLNT VOLITELNÁ, POŽADOVÁNO nebo REQDADM (pokud se připojuje jako administrativní uživatel), je správce front ověřován jménem uživatele a heslem. Správce front zkontroluje operační systém (je-li objekt AUTHINFO typu IDPWOS) nebo úložiště LDAP (je-li objekt AUTHINFO typu IDPWLDAP).

Následující tabulka shrnuje toto chování ověření:

Tabulka 82. Souhrn mechanismů SASL a ověření připojení

Mechanismus SASL	Pověření předávaná z klienta do správce front?	hodnota CHKCLNT
anonymní	Ne	REQUIRED nebo REQDADM-připojení odmítnuto  NONE nebo OPTIONAL-připojení přijato
Obyčejné	Ano, jméno uživatele a heslo	REQUIRED, REQDADM nebo OPTIONAL-jméno uživatele a heslo zkontrolované správcem front  NONE-odmítnuto připojení

Pokud používáte klienta MQ Light , můžete zadat pověření tak, že je zahrnete do adresy AMQP, ke které se připojíte, například:

```
amqp://mwhitehead:mYp4ssw0rd@localhost:5672/sports/football
```

## Nastavení MCAUSER na kanálu

V 8.0.0.4

Kanály AMQP mají atribut MCAUSER, který můžete použít k nastavení ID uživatele produktu IBM MQ , pod kterým jsou všechna připojení k příslušnému kanálu autorizována. Všechna připojení z klientů AMQP do tohoto kanálu přebírají ID MCAUSER, které jste nakonfigurovali. Toto ID uživatele se používá pro ověřování systému zpráv v různých tématech.

Chcete-li zabezpečit připojení ke správcům front, doporučuje se použít ověření kanálu (CHLAUTH). Používáte-li ověřování kanálu, doporučuje se konfigurovat hodnotu MCAUSER na neprivilegovaného uživatele. Tím je zajištěno, že pokud připojení ke kanálu neodpovídá pravidlu CHLAUTH, nebude připojení povoleno provádět žádné zprávy ve správci front.

## Podpora šifrování protokolu

Kanály AMQP podporují šifrování SSL/TLS pomocí klíčů z úložiště klíčů nakonfigurovaného pro vašeho správce front. Volby konfigurace kanálu AMQP pro šifrování SSL/TLS podporují stejné volby jako jiné typy kanálu MQ ; můžete zadat specifikaci šifry a to, zda správce front vyžaduje certifikáty z připojení klienta AMQP.

Pomocí atributů standardu FIPS správce front můžete řídit sady šifer SSL/TLS, které lze použít k zabezpečení připojení z klientů AMQP.

Informace o tom, jak nastavit úložiště klíčů pro správce front, najdete v tématu [Práce s SSL nebo TLS na systémech UNIX, Linux a Windows](#).

Informace o tom, jak nakonfigurovat podporu SSL/TLS pro připojení klienta AMQP, najdete v tématu [Vytvoření a použití kanálů AMQP](#).

### Související informace

[Vyvíjení klientských aplikací AMQP](#)

[Vytvoření a použití kanálů AMQP](#)

Je-li vytvořeno připojení klienta AMQP, které má stejný identifikátor klienta jako existující připojení klienta AMQP, bude při výchozím nastavení odpojeno existující připojení klienta. Správce front však můžete nakonfigurovat tak, aby omezoval chování převzetí klienta tak, aby převzetí bylo možné pouze v případě, že jsou splněna určitá kritéria.

Například odpojení existujícího připojení klienta nemusí být vhodné, pokud existují aplikace AMQP vyvíjeny různými týmy a že používají stejné ID klienta. Chcete-li tento problém vyřešit, můžete omezit převzetí klienta na základě názvu používaného kanálu AMQP, adresy IP klienta a ID uživatele klienta (je-li povoleno ověření SASL).

Použijte nastavení atributů správce front **AdoptNewMCA** a **AdoptNewMCACheck** k uvedení požadované úrovně omezení převzetí klienta, jak je podrobně uvedeno v následující tabulce:

*Tabulka 83. Nastavení **AdoptNewMCA** a **AdoptNewMCACheck** pro omezení převzetí klienta*

<b>AdoptNewMCA</b>	<b>AdoptNewMCACheck</b>	<b>Kritéria zkontrovaná před povolením převzetí klienta</b>
NO nebo nedefinováno	Nelze použít	Není. Převzetí klienta je povoleno pro všechna ověření klienta, která jsou ověřena a předávají všechna pravidla CHLAUTH.
ALL (nebo hodnota jiná než NO)	QM nebo nedefinováno	Není. Převzetí klienta je povoleno pro všechna ověření klienta, která jsou ověřena a předávají všechna pravidla CHLAUTH.
ALL (nebo hodnota jiná než NO)	NAME	ID uživatele (je-li SASL povoleno) Název kanálu
ALL (nebo hodnota jiná než NO)	ADDRESS	ID uživatele (je-li SASL povoleno) Adresa IP
ALL (nebo hodnota jiná než NO)	ALL	ID uživatele (je-li SASL povoleno) Název kanálu Adresa IP

Atributy správce front **AdoptNewMCA** a **AdoptNewMCACheck** jsou součástí konfigurace správce front, která je definována ve stanze CHANNELS. V systémech IBM MQ pro systémy Windows a IBM MQ pro systémy Linux x86-64 upravte informace o konfiguraci pomocí konzoly MQ Explorer. V jiných systémech upravte informace úpravou konfiguračního souboru `qm.ini`. Informace o tom, jak upravit informace o kanálech správce front, najdete v tématu [Atributy stanzy kanálů](#).

### Související informace

[Vyvíjení klientských aplikací AMQP](#)

[Vytvoření a použití kanálů AMQP](#)

## IBM MQ Advanced Message Security

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

## Přehled produktu IBM MQ AMS

Aplikace produktu IBM MQ mohou používat produkt IBM 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 informace

Návratové kódy GSKit použité ve zprávách produktu AMS

### Chování, které se změnilo od Verze 7.0.1

Produkt IBM MQ Advanced Message Security se stal komponentou produktu IBM MQ z produktu Verze 7.5. Některé aspekty funkcí produktu IBM MQ AMS se změnilo, což může mít vliv na aplikace, administrativní skripty nebo procedury správy.

Před upgradem správců front na produkt Verze 7.5 nebo vyšší zkontrolujte následující seznam změn pečlivě. Rozhodněte se, zda musíte naplánovat provedení změn v existujících aplikacích, skriptech a procedurách před spuštěním migrace systémů:

- Instalace produktu IBM MQ AMS je součástí instalačního procesu produktu IBM MQ .
- Schopnost zabezpečení produktu IBM MQ AMS je povolena při její instalaci a je řízena zásadami zabezpečení. Chcete-li povolit, aby produkt IBM MQ AMS zakročoval data, není třeba zachytávat zachytávače.
- Produkt IBM MQ AMS v produktu IBM MQ nevyžaduje použití příkazu **cfgmq** jako v samostatné verzi produktu IBM WebSphere MQ Advanced Message Security.

### Vlastnosti a funkce produktu IBM MQ Advanced Message Security

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

Produkt IBM MQ AMS poskytuje následující funkce:

- Zabezpečuje citlivé nebo vysoce hodnotové transakce zpracovávané produktem IBM MQ.
- Detekuje a odebrá 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 IBM MQ.

### Ošetření chyb

IBM MQ 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 IBM 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.

Produkt IBM MQ Advanced Message Security používá SYSTEM.PROTECTION.ERROR.QUEUE jako frontu zpracování chyb. Všechny zprávy odeslané produktem IBM MQ AMS do systému SYSTEM.PROTECTION.ERROR.QUEUE je předcházena hlavičkou MQDLH.

Administrátor produktu IBM MQ může také definovat SYSTEM.PROTECTION.ERROR.QUEUE jako fronta aliasů odkazující na jinou frontu.

## Klíčové pojmy

Seznamte se s klíčovými koncepty v produktu IBM MQ 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 přidruženém k podepsaným nebo šifrovaným zprávám. Produkt IBM MQ 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 465

K zajištění transparentní kryptografické ochrany pro aplikace IBM MQ používá produkt IBM MQ Advanced Message Security soubor úložiště klíčů, kde jsou uloženy certifikáty veřejných klíčů a soukromý klíč. V systému z/OSse místo souboru úložiště klíčů používá svazek klíčů SAF.

### **digitální certifikáty**

Produkt IBM MQ 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 IBM MQ Advanced Message Security podporuje certifikáty s vlastním podpisem v produktu Java i v nativních aplikacích

## Související informace

[Šifrování](#)

## **Správce oprávnění k objektu**

Na jiných platformách než z/OS je produkt Object Authority Manager (OAM) součástí komponenty služby autorizace dodávané s produkty IBM MQ .

Přístup k entitám IBM MQ Advanced Message Security je řízen pomocí skupin uživatelů produktu IBM MQ a OAM. Administrátoři mohou podle potřeby udělovat nebo odvolávat autorizace pomocí rozhraní příkazového řádku. Různé skupiny uživatelů mohou mít různé druhy přístupových oprávnění ke stejným objektům. Jedna skupina může například provádět operace PUT i GET pro určitou frontu, zatímco jiná skupina může být povolena pouze k procházení fronty. Podobně některé skupiny mohou mít k frontě oprávnění GET a PUT, ale nemohou ji měnit ani odstraňovat.

Prostřednictvím OAM můžete řídit:

- Přístup k objektům produktu IBM MQ 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 informace

[Správce oprávnění k objektu](#)

## **Podporovaná technologie**

Produkt IBM MQ Advanced Message Security závisí na několika technologických komponentách, které zajišťují infrastrukturu zabezpečení.

Produkt IBM MQ Advanced Message Security podporuje následující rozhraní API (Application Programming Interface) produktu IBM MQ :

- Message Queue Interface (MQI)
- IBM MQ Java Message Service (JMS) 1.0.2 a 1.1.
- IBM MQ Základní třídy pro Java
- Třídy IBM MQ pro .Net v nespravovaném režimu

**Poznámka:** Produkt IBM MQ Advanced Message Security podporuje certifikační autority odpovídající standardu X.509 .

## **Známa omezení.**

Informace o omezeních produktu IBM MQ Advanced Message Security.

- Následující volby IBM 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 .

- IBM MQ classes for .NET ve spravovaném režimu (připojení klienta nebo vazby).
- Klient produktu Message Service pro aplikace produktu .NET (XMS).
- Klient Message Service pro aplikace C/C++ (XMS supportPac IA94).
- Fronty produktu IBM MQ zpracovávané pomocí mostu IMS .

**Poznámka:** Produkt IBM MQ AMS je podporován ve frontách produktu CICS Bridge. Stejně ID uživatele byste měli použít pro MQPUT (encrypt) a MQGET (decrypt) na frontách přemostění CICS .

- Všechny aplikace Java jsou závislé na produktu IBM Java Runtime. Produkt IBM MQ AMS nepodporuje žádné prostředí JRE poskytované jinými dodavateli.
- Uživatelé by se měli vyhnout vložení dvou nebo více certifikátů se stejnými rozlišujícími názvy v jednom souboru úložiště klíčů, protože zachytávač IBM MQ AMS s takovými certifikáty není definován.
- Produkt IBM MQ AMS není podporován v produktu JMS , pokud je vlastnost **WMQ\_PROVIDER\_VERSION** nastavena na hodnotu 6.

## Uživatelské scénáře

Seznamte se s možnými scénáři a seznamte se s obchodními cíli, které lze dosáhnout pomocí produktu IBM MQ Advanced Message Security.

### **Stručná úvodní příručka pro produkt IBM MQ AMS na platformách Windows**

Pomocí této příručky můžete rychle nakonfigurovat produkt IBM MQ Advanced Message Security tak, aby poskytoval zabezpečení zpráv na platformách Windows . Po dokončení této operace jste vytvořili databázi klíčů k ověření identit uživatelů a definované zásady podepisování a šifrování pro správce front.

## Než začnete

V systému by měly být nainstalovány alespoň následující funkce:

- Server
- Development Toolkit (pro vzorové programy)
- Advanced Message Security

Podrobné informace naleznete v tématu [Funkce produktu IBM MQ pro systémy Windows](#) .

Informace o použití příkazu **setmqenv** k inicializaci aktuálního prostředí tak, aby příslušné příkazy produktu IBM MQ mohly být umístěny a spuštěny operačním systémem, viz [setmqenv](#).

### 1. Vytvoření správce front a fronty

## Informace o této úloze

Všechny následující příklady používají frontu s názvem TEST . Q pro předávání zpráv mezi aplikacemi. Produkt IBM MQ Advanced Message Security používá zachytávače k podepisování a šifrování zpráv v místě, ve kterém vstupují do infrastruktury produktu IBM MQ prostřednictvím standardního rozhraní produktu IBM MQ . Základní nastavení se provádí v produktu IBM MQ a je konfigurováno v následujících krocích.

Pomocí produktu MQ Explorer můžete vytvořit správce front QM\_VERIFY\_AMS a jeho lokální frontu s názvem TEST . Q tak, že použijete všechna výchozí nastavení průvodce, nebo můžete použít příkazy nalezené v C:\Program Files\IBM\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 `HOME_PATH` 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 vytvořeni a požadovaná oprávnění jim byla udělena.

### Jak pokračovat dále

Chcete-li ověřit, zda byly kroky provedeny správně, použijte ukázky `amqspout` a `amqsget`, jak je popsáno v části [“7. Testování nastavení”](#) na stránce 446.

## 3. Vytvoření databáze klíčů a certifikátů

### Informace o této úloze

Zachytávač vyžaduje veřejný klíč odesílajícího uživatele k zašifrování zprávy. Proto musí být vytvořena klíčová databáze identit uživatelů namapovaných na veřejné a soukromé klíče. V reálném systému, kde uživatelé a aplikace jsou rozptýleni přes několik počítačů, by měl každý uživatel své vlastní soukromé úložiště klíčů. Podobně v této příručce vytváříme databáze klíčů pro `alice` a `bob` a sdílíme uživatelské certifikáty mezi nimi.



**Poznámka:** V této příručce používáme vzorové aplikace napsané v C, které se připojují pomocí lokálních vazeb. Plánujete-li používat aplikace produktu Java s použitím vazeb klienta, je nutné vytvořit úložiště klíčů a certifikáty JKS pomocí příkazu **keytool**, který je součástí prostředí JRE (další podrobnosti viz [“Stručná úvodní příručka pro IBM MQ AMS s klienty Java”](#) na stránce 453). Kroky v této příručce jsou správné pro všechny ostatní jazyky a pro aplikace Java používající lokální vazby.

## Postup

1. Použijte grafické rozhraní Správa klíčů produktu IBM (`strmqikm.exe`) chcete-li vytvořit novou databázi klíčů pro uživatele `alice`.

```
Type: CMS
Filename: alicekey.kdb
Location: C:/Documents and Settings/alice/AMS
```

### Poznámka:

- Je vhodné použít silné heslo k zabezpečení databáze.
  - Ujistěte se, že je vybráno zaškrtnuté políčko **Stash password to a file**.
2. Změňte zobrazení obsahu databáze klíčů na **Osobní certifikáty**.
  3. Vyberte volbu **Nový samopodepsaný**; v tomto scénáři se používají certifikáty s vlastním podpisem.
  4. Vytvořte certifikát identifikující uživatele `alice` pro použití v šifrování pomocí těchto polí:

```
Key label: Alice_Cert
Common Name: alice
Organisation: IBM
Country: GB
```

### Poznámka:

- Pro účely této příručky používáme certifikát podepsaný držitelem, který může být vytvořen bez použití certifikační autority. U výrobních systémů se doporučuje nepoužívat certifikáty podepsané sebou samým, ale spíše spoléhat na certifikáty podepsané vydavatelem certifikátů.
  - Parametr **Key label** určuje název certifikátu, který zachytávače vyhledají, aby obdrželi potřebné informace.
  - Parametry **Common Name** a nepovinné parametry uvádí podrobnosti o **rozlišujícím názvu** (DN), které musí být jedinečné pro každého uživatele.
5. Opakovat krok 1-4 pro uživatele `bob`

## Výsledky

Dva uživatelé `alice` a `bob` mají každý nyní certifikát podepsaný svým držitelem.

### 4. Vytvoření souboru `keystore.conf`

## Informace o této úloze

Musíte zadat IBM MQ Advanced Message Security zachytávačů do adresáře, kde jsou klíčové databáze a certifikáty `located.This` se provádí prostřednictvím souboru `keystore.conf`, který obsahuje tyto informace ve formě prostého textu. Každý uživatel musí mít samostatný soubor `keystore.conf` ve složce `.mqs`. Tento krok musí být proveden jak pro `alice`, tak pro `bob`.

Obsah produktu `keystore.conf` musí být ve tvaru:

```
cms.keystore = <dir>/keystore_file
cms.certificate = certificate_label
```

## Příklad

Pro tento scénář bude obsah souboru `keystore.conf` následující:

```
cms.keystore = C:/Documents and Settings/alice/AMS/alicekey
cms.certificate = Alice_Cert
```

## Poznámka:

- Cesta k souboru úložiště klíčů musí být poskytnuta bez přípony souboru.
- Návěští certifikátu může obsahovat mezery, tedy "Alice\_Cert" a "Alice\_Cert" (s prostorem na konci) například jsou rozpoznány jako popisky dvou různých certifikátů. Aby se však předešlo nejasnostem, je lepší nepoužívat mezery v názvu návěští.
- K dispozici jsou následující formáty úložiště klíčů: CMS (Syntaxe kryptografických zpráv), JKS (Java Úložiště klíčů) a JCEKS (Java Cryptographic Extension Keystore). Další informace jsou uvedeny v tématu [“Struktura konfiguračního souboru úložiště klíčů \(keystore.conf\) pro AMS”](#) na stránce 466.
- `%HOMEDRIVE%\%HOMEPATH%\ .mqs\keystore.conf` (např. `C:\Documents and Settings\alice\.mqs\keystore.conf`) je výchozí umístění, kde IBM MQ 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 465.
- Chcete-li vytvořit adresář `.mqs`, musíte použít příkazový řádek.

## 5. Sdílení certifikátů

### Informace o této úloze

Sdílejte certifikáty mezi dvěma klíčovými databázemi tak, aby každý uživatel mohl úspěšně identifikovat ostatní. To se provádí extrahováním veřejného certifikátu každého uživatele do souboru, který je poté přidán do databáze klíčů druhého uživatele.

**Poznámka:** Dávejte pozor, abyste použili volbu `extract`, a ne volbu `export`. Volba *Extrahovat* získá veřejný klíč uživatele, zatímco `export` získá veřejný i soukromý klíč. Použití `exportu` omylem by zcela ohrozilo vaši aplikaci tím, že se předá na soukromý klíč.

## Postup

1. Extrahujte certifikát identifikující alice do externího souboru:

```
runmqakm -cert -extract -db "C:/Documents and Settings/alice/AMS/alicekey.kdb" -pw passw0rd
-label Alice_Cert -target alice_public.arm
```

2. Přidejte certifikát do úložiště klíčů produktu bob 's :

```
runmqakm -cert -add -db "C:/Documents and Settings/bob/AMS/bobkey.kdb" -pw passw0rd -label
Alice_Cert -file alice_public.arm
```

3. Opakujte kroky pro bob:

```
runmqakm -cert -extract -db "C:/Documents and Settings/bob/AMS/bobkey.kdb" -pw passw0rd
-label Bob_Cert -target bob_public.arm

runmqakm -cert -add -db "C:/Documents and Settings/alice/AMS/alicekey.kdb" -pw passw0rd
-label Bob_Cert -file bob_public.arm
```

## Výsledky

Dva uživatelé alice a bob se nyní mohou navzájem úspěšně identifikovat, protože vytvořili a sdíleli certifikáty podepsané sebou samým.

## Jak pokračovat dále

Ověřte, že je certifikát v úložišti klíčů buď tím, že jej prohledáním pomocí grafického rozhraní, nebo spuštěním následujících příkazů, které vytisknou jeho podrobnosti:

```
runmqkm -cert -details -db "C:/Documents and Settings/bob/AMS/bobkey.kdb" -pw passwd -label Alice_Cert
```

```
runmqkm -cert -details -db "C:/Documents and Settings/alice/AMS/alicekey.kdb" -pw passwd -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 `setmqsp1`. Další informace o tomto příkazu najdete v souboru `setmqsp1`. 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:

```
setmqsp1 -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:

```
dspmqsp1 -m QM_VERIFY_AMS
```

Chcete-li vytisknout podrobnosti o zásadě jako sadu příkazů `setmqsp1`, parametr `-export`. To umožňuje ukládání již definovaných zásad:

```
dspmqsp1 -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 bob procházejte zprávou s použitím ukázkové aplikace přes alias fronty tentokrát:

```
amqsbcg TEST.ALIAS QM_VERIFY_AMS
```

5. Jako uživatel bob získajte 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 IBM MQ AMS v systému SYSTÉM UNIX

Pomocí této příručky můžete rychle nakonfigurovat produkt IBM MQ Advanced Message Security tak, aby poskytoval zabezpečení zpráv produktu SYSTÉM 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:

- Běžové prostředí
- Server
- Ukázkové programy.
- IBM Sada globálního zabezpečení
- MQ Advanced Message Security

Názvy komponent na každé specifické platformě naleznete v následujících tématech:

- [Komponenty produktu IBM MQ pro systémy Linux](#)
- [Komponenty produktu IBM MQ pro systémy HP-UX](#)
- [Komponenty produktu IBM MQ pro systémy AIX](#)
- [Komponenty produktu IBM 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. Produkt IBM MQ Advanced Message Security používá zachytávače k podepisování a šifrování zpráv v místě, ve kterém vstupují do infrastruktury produktu IBM MQ prostřednictvím standardního rozhraní produktu IBM MQ . Základní nastavení se provádí v produktu IBM MQ a je konfigurováno v následujících krocích.

Pomocí produktu IBM MQ Explorer můžete vytvořit správce front QM\_VERIFY\_AMS a jeho lokální frontu s názvem TEST . Q tak, že použijete všechna výchozí nastavení průvodce, nebo můžete použít příkazy nalezené v <MQ\_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 `amqspout` a `amqsget`, jak je popsáno v části [“8. Testování šifrování”](#) na stránce 453.

#### 3. Vytvoření databáze klíčů a certifikátů

### Informace o této úloze

Pro zašifrování zprávy zachytávač vyžaduje soukromý klíč odesilajícího uživatele a veřejný klíč (y) příjemce (ů). Proto musí být vytvořena klíčová databáze identit uživatelů namapovaných na veřejné a soukromé klíče. V reálném systému, kde uživatelé a aplikace jsou rozptýleni přes několik počítačů, by měl každý uživatel své vlastní soukromé úložiště klíčů. Podobně v této příručce vytváříme databáze klíčů pro `alice` a `bob` a sdílíme uživatelské certifikáty mezi nimi.

**Poznámka:** V této příručce používáme vzorové aplikace napsané v C, které se připojují pomocí lokálních vazeb. Plánujete-li používat aplikace produktu Java s použitím vazeb klienta, je nutné vytvořit úložiště klíčů a certifikáty JKS pomocí příkazu **keytool**, který je součástí prostředí JRE (další podrobnosti viz [“Stručná úvodní příručka pro IBM MQ AMS s klienty Java”](#) na stránce 453). 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 passwd -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 nečítelná všichni ostatní uživatelé.

```
chown alice /home/alice/.mqs/alicekey.kdb /home/alice/.mqs/alicekey.sth  
chmod 600 /home/alice/.mqs/alicekey.kdb /home/alice/.mqs/alicekey.sth
```

5. Opakovat krok 1-4 pro uživatele `bob`

## Výsledky

Dva uživatelé `alice` a `bob` mají každý nyní certifikát podepsaný svým držitelem.

4. Vytvoření souboru `keystore.conf`

### Informace o této úloze

Do adresáře, kde jsou umístěny databáze klíčů a certifikáty, musíte zabodávat zachytávače IBM MQ Advanced Message Security. To se provádí prostřednictvím souboru `keystore.conf`, který obsahuje informace v podobě prostého textu. Každý uživatel musí mít samostatný soubor `keystore.conf` ve složce `.mqs`. Tento krok musí být proveden jak pro `alice`, tak pro `bob`.

Obsah produktu `keystore.conf` musí být ve tvaru:

```
cms.keystore = <dir>/keystore_file  
cms.certificate = certificate_label
```

### Příklad

Pro tento scénář bude obsah souboru `keystore.conf` následující:

```
cms.keystore = /home/alice/.mqs/alicekey  
cms.certificate = Alice_Cert
```

### Poznámka:

- Cesta k souboru úložiště klíčů musí být poskytnuta bez přípony souboru.

- K dispozici jsou následující formáty úložiště klíčů: CMS (Syntaxe kryptografických zpráv), JKS (Java Úložiště klíčů) a JCEKS (Java Cryptographic Extension Keystore). Další informace jsou uvedeny v tématu “Struktura konfiguračního souboru úložiště klíčů (keystore.conf) pro AMS” na stránce 466.
- HOME/.mqsc/keystore.conf je výchozí umístění, kde IBM MQ 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 465.

## 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/.mqsc/alicekey.kdb -pw passwd -label Alice_Cert
-target alice_public.arm
```

2. Přidejte certifikát do úložiště klíčů produktu bob 's :

```
runmqakm -cert -add -db /home/bob/.mqsc/bobkey.kdb -pw passwd -label Alice_Cert -file
alice_public.arm
```

3. Zopakujte tento krok pro bob:

```
runmqakm -cert -extract -db /home/bob/.mqsc/bobkey.kdb -pw passwd -label Bob_Cert -target
bob_public.arm
```

4. Add the certificate for bob to alice 's keystore:

```
runmqakm -cert -add -db /home/alice/.mqsc/alicekey.kdb -pw passwd -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/.mqsc/bobkey.kdb -pw passwd -label Alice_Cert
runmqakm -cert -details -db /home/alice/.mqsc/alicekey.kdb -pw passwd -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 setmqsp1.



Další informace o tomto příkazu najdete v souboru `setmqsp1`. 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:

```
setmqsp1 -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:

```
dspmqsp1 -m QM_VERIFY_AMS
```

Chcete-li vytisknout podrobnosti o zásadě jako sadu příkazů `setmqsp1`, parametr `-export`. To umožňuje ukládání již definovaných zásad:

```
dspmqsp1 -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 ukázkový příkaz. 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 `bob` se 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 `bob` procházejte zprávou s použitím ukázkové aplikace přes alias fronty tentokrát:

```
./amqsbcg TEST.ALIAS QM_VERIFY_AMS
```

5. Jako uživatel `bob` získajte 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 IBM MQ AMS s klienty Java

Pomocí této příručky můžete rychle nakonfigurovat produkt IBM MQ Advanced Message Security a poskytnout zabezpečení zpráv pro aplikace produktu Java, které se připojují pomocí vazeb klienta. Po dokončení tohoto procesu jste vytvořili úložiště klíčů k ověření identit uživatelů a definované zásady pro podepisování a šifrování pro správce front.

## Než začnete

Ujistěte se, že máte nainstalované příslušné komponenty, jak je popsáno v **Stručné úvodní příručce** ([Windows](#) nebo [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. Produkt IBM MQ Advanced Message Security používá zachytávače k podepisování a šifrování zpráv v místě, ve kterém vstupují do infrastruktury produktu IBM MQ prostřednictvím standardního rozhraní produktu IBM MQ. Základní nastavení se provádí v produktu IBM MQ a je konfigurováno v následujících krocích.

### Postup

1. Vytvoření správce front

```
crtmqm QM_VERIFY_AMS
```

2. Spustit správce front

```
strmqm QM_VERIFY_AMS
```

3. Vytvořte a spusťte modul listener zadáním následujících příkazů do produktu **runmqsc** pro správce front QM\_VERIFY\_AMS

```
DEFINE LISTENER(AMS.LSTR) TRPTYPE(TCP) PORT(1414) CONTROL(QMGR)  
START LISTENER(AMS.LSTR)
```

4. Vytvořte kanál pro naše aplikace k připojení zadáním následujícího příkazu do produktu **runmqsc** pro správce front QM\_VERIFY\_AMS

```
DEFINE CHANNEL(AMS.SVRCONN) CHLTYPE(SVRCONN)
```

5. Vytvořte frontu s názvem TEST.Q zadáním následujícího příkazu do produktu **runmqsc** pro správce front QM\_VERIFY\_AMS

```
DEFINE QLOCAL(TEST.Q)
```

### Výsledky

Pokud byla procedura úspěšně dokončena, následující příkaz zadaný do produktu **runmqsc** zobrazí podrobnosti o produktu TEST.Q:

```
DISPLAY Q(TEST.Q)
```

## 2. Vytvoření a autorizace uživatelů

### Informace o této úloze

Existují dva uživatelé, kteří se zobrazí v tomto scénáři: **alice**, odesílatel a **bob**, příjemce. K tomu, abyste mohli používat aplikační frontu, je třeba těmto uživatelům udělit oprávnění k jeho používání. Také pro úspěšné použití zásad ochrany definovaných v tomto scénáři musí být těmto uživatelům udělen přístup k některým systémovým frontám. Další informace o příkazu **setmqaut** naleznete v části [setmqaut](#).

### Postup

1. Vytvořte dva uživatele 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 vytvořeni 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 458.

### 3. Vytvoření databáze klíčů a certifikátů

## Informace o této úloze

Chcete-li zašifrovat zprávu zachytávačem, je nutný veřejný klíč odesílajícího uživatele. Proto musí být vytvořena klíčová databáze identit uživatelů namapovaných na veřejné a soukromé klíče. V reálném systému, kde uživatelé a aplikace jsou rozptýleni přes několik počítačů, by měl každý uživatel své vlastní soukromé úložiště klíčů. Podobně v této příručce vytváříme databáze klíčů pro `alice` a `bob` a sdílíme uživatelské certifikáty mezi nimi.

**Poznámka:** V této příručce se používají ukázkové aplikace napsané v produktu Java, které se připojují pomocí vazeb klienta. Plánujete-li používat aplikace produktu Java s použitím lokálních vazeb nebo aplikací v jazyce C, je nutné vytvořit úložiště klíčů a certifikáty CMS pomocí příkazu `runmqakm`. To se zobrazí v **Stručné úvodní příručce** ([Windows](#) nebo [UNIX](#)).

## Postup

1. Vytvořte adresář, ve kterém chcete vytvořit úložiště klíčů, například `/home/alice/.mqsc`. Možná ji budete chtít vytvořit ve stejném adresáři, jaký používá **Stručná úvodní příručka** ([Windows](#) nebo [UNIX](#)) pro vaši platformu.

**Poznámka:** Tento adresář je označován jako `keystore-dir` v následujících krocích

2. Vytvoření nového úložiště klíčů a certifikátu identifikujícího uživatele `alice` pro použití v šifrování

**Poznámka:** Příkaz `keytool` je součástí prostředí JRE.

```
keytool -genkey -alias Alice_Java_Cert -keyalg RSA -keystore keystore-dir/keystore.jks
-storepass passw0rd
-dname "CN=alice, O=IBM, C=GB" -keypass passw0rd
```

### Poznámka:

- Pokud adresář `keystore-dir` obsahuje mezery, je třeba zadat úplný název úložiště klíčů do uvozovek.
- Je vhodné použít silné heslo k zabezpečení úložiště klíčů.
- Pro účely této příručky používáme certifikát podepsaný držitelem, který může být vytvořen bez použití certifikační autority. U výrobních systémů se doporučuje nepoužívat certifikáty podepsané sebou samým, ale spíše spoléhat na certifikáty podepsané vydavatelem certifikátů.
- Parametr `alias` určuje název certifikátu, který zachytávače vyhledají, aby obdrželi potřebné informace.
- Parametr `dname` určuje podrobnosti o **rozlišujícím názvu** (DN), které musí být jedinečné pro každého uživatele.

3. V systému UNIX kontrolujte, zda je úložiště klíčů čitelné.

```
chmod +r keystore-dir/keystore.jks
```

4. Zopakovat step1-4 pro uživatele bob

## Výsledky

Dva uživatelé alice a bob mají každý nyní certifikát podepsaný svým držitelem.

4. Vytvoření souboru *keystore.conf*

## Informace o této úloze

Do adresáře, kde jsou umístěny databáze klíčů a certifikáty, musíte zabodávat zachytávače IBM MQ Advanced Message Security . To se provádí pomocí souboru *keystore.conf* , který uchovává tyto informace ve formě prostého textu. Každý uživatel musí mít samostatný soubor *keystore.conf* . Tento krok by měl být proveden pro alice i pro bob.

## Příklad

Pro tento scénář je obsah souboru *keystore.conf* pro produkt alice následující:

```
JKS.keystore = keystore-dir/keystore
JKS.certificate = Alice_Java_Cert
JKS.encrypted = no
JKS.keystore_pass = passw0rd
JKS.key_pass = passw0rd
JKS.provider = IBMJCE
```

Pro tento scénář je obsah souboru *keystore.conf* pro produkt bob následující:

```
JKS.keystore = keystore-dir/keystore
JKS.certificate = Bob_Java_Cert
JKS.encrypted = no
JKS.keystore_pass = passw0rd
JKS.key_pass = passw0rd
JKS.provider = IBMJCE
```

## Poznámka:

- Cesta k souboru úložiště klíčů musí být poskytnuta bez přípony souboru.
- Pokud již máte soubor *keystore.conf* , protože jste postupovali podle pokynů v příručce Quick Start Guide ( [Windows](#) nebo [UNIX](#) ), můžete upravit existující soubor a přidat tyto řádky.
- Další informace viz [“Struktura konfiguračního souboru úložiště klíčů \(keystore.conf\) pro AMS”](#) na stránce 466.

5. *Sdílení certifikátů*

## Informace o této úloze

Sdílejte certifikáty mezi dvěma úložišti klíčů tak, aby každý uživatel mohl úspěšně identifikovat ostatní. To se provádí extrahováním certifikátu každého uživatele a jeho importem do úložiště klíčů jiného uživatele.

**Poznámka:** Termíny *extract* a *export* se používají rozdílně různými nástroji certifikátů. Nástroj IBM GSKit **strmqikm** (nástroj ikeyman) například rozlišuje, že jste *extrahovali* certifikáty (veřejné klíče) a soukromé klíče *exportu* . Tento rozdíl je nesmírně důležitý pro nástroje, které nabízejí obě možnosti, protože používání *exportu* omylem zcela kompromituje vaši aplikaci předáním svého soukromého klíče. Protože je rozdíl natolik důležitý, snaží se dokumentace produktu IBM MQ důsledně používat tyto termíny. Nástroj keytool produktu Java však poskytuje volbu příkazového řádku s názvem *exportcert* , která extrahuje pouze veřejný klíč. Z těchto důvodů se následující procedura odkazuje na *extrahování* certifikátů pomocí volby *exportcert* .

## Postup

1. Extrahujte certifikát označující *alice*.

```
keytool -exportcert -keystore alice-keystore-dir/keystore.jks -storepass passw0rd
-alias Alice_Java_Cert -file alice-keystore-dir/Alice_Java_Cert.cer
```

2. Importujte certifikát, který identifikuje produkt *alice*, do úložiště klíčů, které bude používat produkt *bob*. Až budete vyzváni, označte, že tomuto certifikátu důvěřujete.

```
keytool -importcert -file alice-keystore-dir/Alice_Java_Cert.cer -alias Alice_Java_Cert
-keystore bob-keystore-dir/keystore.jks -storepass passw0rd
```

3. Zopakujte kroky pro *bob*

## Výsledky

Dva uživatelé *alice* a *bob* se nyní mohou navzájem úspěšně identifikovat, protože vytvořili a sdíleli certifikáty podepsané sebou samým.

## Jak pokračovat dále

Spuštěním následujících příkazů, které vytisknou jeho podrobnosti, ověřte, že je certifikát v úložišti klíčů:

```
keytool -list -keystore bob-keystore-dir/keystore.jks -storepass passw0rd -alias Alice_Java_Cert
keytool -list -keystore alice-keystore-dir/keystore.jks -storepass passw0rd -alias Bob_Java_Cert
```

## 6. Definování zásady fronty

### Informace o této úloze

Se správcem front vytvořeným a zachytávačem připraveným k zachycení zpráv a přístupu k šifrovacím klíčům můžeme začít definovat zásady ochrany na systému `QM_VERIFY_AMS` pomocí příkazu `setmqsp1`. Další informace o tomto příkazu najdete v souboru `setmqsp1`. 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*:

```
setmqsp1 -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:

```
dspmqsp1 -m QM_VERIFY_AMS
```

Chcete-li vytisknout podrobnosti o zásadě jako sadu příkazů `setmqsp1`, parametr `-export`. To umožňuje ukládání již definovaných zásad:

```
dspmqsp1 -m QM_VERIFY_AMS -export >restore_my_policies.bat
```

## 7. Testování nastavení

### Než začnete

Ujistěte se, že verze jazyka Java, kterou používáte, má nainstalované neomezené soubory zásad JCE.

**Poznámka:** Verze jazyka Java dodaná v instalaci produktu IBM MQ již má tyto soubory zásad. Lze jej nalézt v `MQ_INSTALLATION_PATH/java/bin`.

### Informace o této úloze

Spuštěním různých programů pod různými uživateli můžete ověřit, zda byla aplikace řádně nakonfigurována. Další informace naleznete v **Stručné úvodní příručce** ([Windows](#) nebo [UNIX](#)) pro vaši platformu, kde získáte podrobnosti o spuštění programů pod různými uživateli.

### Postup

1. Chcete-li spustit tyto ukázkové aplikace produktu JMS, použijte nastavení CLASSPATH pro vaši platformu, jak je zobrazeno v tématu [Proměnné prostředí používané produktem IBM MQ classes for JMS](#) k zajištění toho, aby byl zahrnut adresář ukázek.
2. Jako uživatel alice vložte zprávu s použitím ukázkové aplikace, která se připojuje jako klient:

```
java JMSProducer -m QM_VERIFY_AMS -d TEST.Q -h localhost -p 1414 -l AMS.SVRCONN
```

3. Jako uživatel bob získám 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 IBM MQ Advanced Message Security zadrží operaci a zpracuje zprávu na základě sady zásad pro vzdálenou frontu. Například pro zásadu šifrování je zpráva zašifrována před tím, než je předána procesu IBM MQ, aby se s ní ošetla. Poté, co příkaz IBM MQ Advanced Message Security zpracoval zprávu vdanou do vzdálené fronty, vloží příkaz IBM MQ do přidružené přenosové fronty a předá ji cílovému správci front a cílové frontě.

Je-li operace GET provedena v lokální frontě, produkt IBM MQ Advanced Message Security se pokusí dekodovat zprávu podle sady zásad v lokální frontě. Aby byla operace úspěšná, musí být zásada použita k dešifrování zprávy identická s tím, která byla použita k zašifrování. Jakýkoli nesoulad způsobí, že zpráva bude odmítnuta.

Pokud z nějakého důvodu nemohou být obě zásady nastaveny současně, je poskytována podpora fázovaného nasazení. Zásada může být nastavena na lokální frontě s příznakem tolerování, což znamená, že zásada přidružená k frontě může být ignorována, když se pokus o načtení zprávy z fronty zahrnuje zprávu, která nemá nastavovanou sadu zásad zabezpečení. V takovém případě se metoda GET pokusí dešifrovat zprávu, ale umožní doručení nešifrovaných zpráv. Takto mohou být zásady vzdálených front nastaveny po ochraně lokálních front (a testování).

**Zapamatujte si:** Jakmile je dokončeno ukončení IBM MQ Advanced Message Security, odeberte příznak tolerance.

### Související odkazy

[setmqspl \(nastavit zásady zabezpečení\)](#)

## Směrování chráněných zpráv pomocí IBM Integration Bus

Produkt IBM MQ Advanced Message Security může ochraňovat zprávy v infrastruktuře, kde je nainstalován produkt IBM Integration Bus nebo produkt WebSphere Message Broker verze Verze 8.0.0.1 (nebo novější). Před použitím zabezpečení v prostředí produktu IBM Integration Bus byste měli porozumět povaze obou produktů.

### Informace o této úloze

IBM MQ Advanced Message Security poskytuje konec pro zabezpečení informačního obsahu zprávy. To znamená, že pouze účastníci uvedení jako platní odesílatelé a příjemci zprávy jsou schopni produkovat nebo přijímat. To znamená, že za účelem zabezpečení zpráv procházejících přes IBM Integration Bus můžete buď povolit IBM Integration Bus ke zpracování zpráv, aniž byste znali jejich obsah ( [Scénář 1](#) ) nebo jej zpřístupníte autorizovaným uživatelem pro příjem a odesílání zpráv ( [Scénář 2](#) ).

*Scénář 1 - Integration Bus nemůže zobrazit obsah zprávy*

### Než začnete

Měli byste mít IBM Integration Bus připojený ke stávajícímu správci front. Řetězec `QMGrName` nahradte 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 `routeTo` je zpráva směrována buď na `bob's` ( QBOB ),<sup>1</sup> ( QCECIL ) nebo výchozí fronty ( QDEF ). Směrování je možné, protože IBM MQ Advanced Message Security chrání pouze informační obsah zprávy a ne jeho záhlaví a vlastnosti, které zůstávají nechráněné a mohou být čteny IBM Integration Bus. Produkt IBM MQ Advanced Message Security používá pouze `alice`, `bob` a `cecil`. Není nutné ji instalovat nebo konfigurovat pro produkt IBM Integration Bus.

Produkt IBM Integration Bus přijme chráněnou zprávu z nezabezpečené fronty aliasů, aby nedošlo k pokusu o dešifrování zprávy. Pokud by se jednalo o přímé použití chráněné fronty, zpráva by byla vložena do fronty DEAD LETTER jako nemožnou k dešifrování. Zpráva je směrována IBM Integration Bus a je doručena do cílové fronty nezměněná. Proto je i nadále podepsán původním autorem (oba `bob` a `cecil` přijímají pouze zprávy odeslané `alice` ) a chráněné jako předtím (pouze `bob` a `cecil` mohou číst). Příkaz IBM Integration Bus vloží přesměrovanou zprávu do nechráněného aliasu. Příjemci načtou zprávu z chráněné výstupní fronty, kde IBM MQ AMS transparentně dešifruje zprávu.

### Postup

1. Nakonfigurujte `alice`, `bob` a `cecil` pro použití produktu IBM MQ 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 úložiště 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.

---

<sup>1</sup> 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 odesílatel 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 IBM Integration Bus vytvořte tok zpráv pro směrování zpráv, které přicházejí do fronty aliasů AIN , do uzlu BOB, CECIL nebo DEF v závislosti na vlastnosti `routeTo` zprávy. Chcete-li to provést:

- Vytvořte uzel MQInput s názvem IN a přiřadte mu alias AIN jako název fronty.
- Vytvořte uzly MQOutput s názvem BOB, CECIL a DEF a přiřadte aliasy front ABOB, ACECIL a ADEF jako příslušné názvy front.
- Vytvořte uzel přenosové cesty a nazveť je TEST.
- Připojte uzel IN ke vstupnímu terminálu uzlu TEST .
- Vytvořte výstupní terminály boba `cecil` pro uzel TEST .
- Připojte výstupní terminál `bob` k uzlu BOB .
- Připojte výstupní terminál `cecil` k uzlu CECIL .
- Připojte uzel DEF k výchozímu výstupnímu terminálu.
- Použijte následující pravidla:

```
$Root/MQRFH2/usr/routeTo/text()="bob"  
$Root/MQRFH2/usr/routeTo/text()="cecil"
```

9. Implementujte tok zpráv do běhové komponenty produktu IBM Integration Bus .
10. Spuštění jako uživatel Alice vložil zprávu, která také obsahuje vlastnost zprávy s názvem `routeTo` s hodnotou buď `bob` , nebo `cecil`. Spuštění ukázkové aplikace **amqsstm** vám umožní toto provést.

```
Sample AMQSSTMA start  
target queue is TEST.Q  
Enter property name  
routeTo  
Enter property value  
bob  
Enter property name  
  
Enter message text  
My Message to Bob  
Sample AMQSSTMA end
```

11. Při spuštění jako uživatel *bob* načtěte zprávu z fronty QBOB s použitím ukázkové aplikace **amqsget**.

## Výsledky

Když text *alice* vloží zprávu do fronty *QIN*, je zpráva chráněna. Je načten v chráněné formě produktem IBM Integration Bus z alias fronty *AIN*. IBM Integration Bus rozhoduje o tom, kam směřovat zprávu při čtení vlastnosti *routeTo*, která je jako všechny vlastnosti nešifrována. Produkt IBM Integration Bus umístí zprávu na příslušný nechráněný alias, aby se zabránilo jeho další ochraně. Při přijetí od *bob* nebo *cecil* z fronty je zpráva dešifrována a digitální podpis je ověřen.

*Scénář 2- Integration Bus může zobrazit obsah zprávy*

## Informace o této úloze

V tomto scénáři je skupině jednotlivců povoleno odesílat zprávy do produktu IBM Integration Bus. Jiná skupina je oprávněna přijímat zprávy, které jsou vytvořeny produktem IBM Integration Bus. Přenos mezi stranami a IBM Integration Bus nemůže být odposlouchněný.

Pamatujte, že produkt IBM Integration Bus čte zásady ochrany a certifikáty pouze při otevření fronty, takže musíte znovu načíst skupinu provádění po provedení jakýchkoli aktualizací zásad ochrany, aby změny nabyly platnosti.

```
mqsireload execution-group-name
```

Je-li produkt IBM Integration Bus považován za autorizovanou stranu, která má oprávnění ke čtení nebo podepsání informačního obsahu zprávy, musíte nakonfigurovat prostor IBM MQ Advanced Message Security pro uživatele spouštějícího službu IBM Integration Bus. Mějte na paměti, že se nejedná nutně o stejného uživatele, který vkládá/získává zprávy do front, ani uživatele, který vytváří a implementuje aplikace produktu IBM Integration Bus.

## Postup

1. Nakonfigurujte *alice*, *bob*, *cecil* a *dave* a uživatele služby IBM Integration Bus, abyste mohli použít produkt IBM MQ 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* uživateli služeb produktu IBM Integration Bus.

To provedete extrakcí každého z certifikátů, které identifikují *alice*, *bob*, *cecil* a *dave*, do externích souborů a poté přidají extrahované certifikáty do úložiště klíčů produktu IBM Integration Bus. Je důležité, abyste použili metodu popsanou v **Úloha 5. Sdílení certifikátů** v příručce **Quick Start Guide** ([Windows](#) nebo [UNIX](#)).

3. Zadejte certifikát uživatele služby IBM Integration Bus do *alice*, *bob*, *cecil* a *dave*.

Postupujte takto s použitím metody uvedené v předchozím kroku.

**Poznámka:** *Alice* a *bob* potřebují certifikát uživatele služby IBM Integration Bus, aby správně zašifrovali zprávy. Uživatel služby IBM Integration Bus potřebuje certifikáty *alice's* a *bob* k ověření autorů zpráv. Uživatel služby IBM Integration Bus potřebuje certifikáty *cecil's* a *dave*, aby pro ně šifroval zprávy. *cecil* a *dave* potřebují certifikát uživatele služby IBM Integration Bus, aby ověřil, zda zpráva pochází z produktu IBM Integration Bus.

4. Definujte lokální frontu s názvem *IN* a definujte zásadu zabezpečení s hodnotou *alice* a *bob* určeným jako autoři a uživatel služby pro IBM Integration Bus zadaný jako příjemce:

```
setmqsp1 -m QMgrName -p IN -s MD5 -a "CN=alice,O=IBM,C=GB" -a "CN=bob,O=IBM,C=GB"  
-e AES256 -r "CN=broker,O=IBM,C=GB"
```

5. Definujte lokální frontu s názvem OUT a definujte zásadu zabezpečení se servisním uživatelem pro IBM Integration Bus zadanou jako autor a *cecil* a *dave* uvedeným jako příjemci:

```
setmqspl -m QMgrName -p OUT -s MD5 -a "CN=broker,O=IBM,C=GB" -e AES256  
-r "CN=cecil,O=IBM,C=GB" -r "CN=dave,O=IBM,C=GB"
```

6. V produktu IBM Integration Bus vytvořte tok zpráv s uzlem MQInput a MQOutput . Nakonfigurujte uzel MQInput pro použití fronty IN a uzlu MQOutput pro použití fronty OUT .
7. Implementujte tok zpráv do běhové komponenty produktu IBM Integration Bus .
8. Spuštění jako uživatel *alice* nebo *bob* vloží zprávu do fronty IN s použitím ukázkové aplikace **amqspmt**.
9. Při spuštění jako uživatel *cecil* nebo *dave* načtete zprávu z fronty OUT s použitím ukázkové aplikace **amqsget**.

## Výsledky

Zprávy odeslané pomocí *alice* nebo *bob* do vstupní fronty IN jsou šifrovány tak, že je lze číst pouze IBM Integration Bus . Produkt IBM Integration Bus přijímá pouze zprávy od *alice* a *bob* a odmítá všechny ostatní. Přijímané zprávy jsou odpovídajícím způsobem zpracovány, pak jsou podepsány a šifrovány pomocí klíčů *cecil* a *dave* před tím, než jsou vloženy do výstupní fronty OUT. Pouze *cecil* a *dave* jsou schopny je číst, zprávy, které nejsou podepsány IBM Integration Bus , jsou zamítnuty.

## Použití IBM MQ AMS s IBM MQ Managed File Transfer

Tento scénář vysvětluje, jak nakonfigurovat produkt IBM MQ Advanced Message Security , aby poskytl utajení zpráv pro data odesílaná prostřednictvím IBM MQ Managed File Transfer.

## Než začnete

Ujistěte se, že máte nainstalovanou komponentu IBM MQ Advanced Message Security v rámci instalace produktu IBM MQ , která je hostitelem front používaných produktem IBM MQ Managed File Transfer , které chcete chránit.

Pokud se vaši agenti IBM MQ Managed File Transfer připojují v režimu vazeb, ujistěte se, že máte také nainstalovanou komponentu GSKit na lokální instalaci.

## Informace o této úloze

Je-li přenos dat mezi dvěma agenty IBM MQ Managed File Transfer přerušen, potenciálně důvěrné údaje mohou zůstat nechráněny na základních frontách produktu IBM MQ používaných ke správě přenosu. Tento scénář vysvětluje, jak nakonfigurovat a používat produkt IBM MQ Advanced Message Security k ochraně těchto dat ve frontách produktu IBM MQ Managed File Transfer .

V tomto scénáři uvažujeme jednoduchou topologii zahrnující jeden počítač se dvěma frontami IBM MQ Managed File Transfer a dvěma agenty, AGENT1 a AGENT2a sdílením jednoho správce front, jak je popsáno v tématu [Přehled scénáře](#). Oba agenti se připojují stejným způsobem, buď v režimu vazeb, nebo v režimu klienta.

### 1. Vytvoření certifikátů

## Než začnete

Tento scénář používá jednoduchý model, kde se uživatel *ftagent* ve skupině FTAGENTS používá ke spuštění procesů agenta IBM MQ Managed File Transfer . Pokud používáte vlastní názvy uživatelů a skupin, změňte odpovídajícím způsobem příkazy.

## Informace o této úloze

Produkt IBM MQ Advanced Message Security používá šifrování pomocí veřejného klíče k podpisu a/nebo šifrování zpráv v chráněných frontách.

## Poznámka:

- Pokud jsou agenti IBM MQ Managed File Transfer spuštěni v režimu vazeb, příkazy, které používáte k vytvoření úložiště klíčů CMS (Cryptographic Message Syntax), jsou podrobně popsány v **Stručné úvodní příručce** ( Windows nebo UNIX ) pro vaši platformu.
- Pokud jsou agenti IBM MQ Managed File Transfer spuštěni v režimu klienta, příkazy, které budete potřebovat pro vytvoření JKS ( Java Keystore), jsou podrobně popsány v [“Stručná úvodní příručka pro IBM MQ AMS s klienty Java”](#) na stránce 453.

## 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 **setmqsp1** . 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 MQ Managed File Transfer v rámci přípravy na ochranu pomocí příkazu **fteStopAgent** .
2. Vytvoření zásad zabezpečení pro ochranu fronty `SYSTEM.FTE.DATA.AGENT2` .

```
setmqsp1 -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 spouští proces agenta IBM MQ Managed File Transfer , má přístup k procházení fronty zásad systému a vloží zprávy do fronty chyby.

```
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 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.

## instalace IBM MQ Advanced Message Security

Nainstalujte komponentu produktu IBM MQ Advanced Message Security na různých platformách.

## Informace o této úloze

Kompletní instalační procedury naleznete v tématu [Instalace produktu IBM MQ Advanced Message Security](#) .

## Související informace

[Odinstalace IBM MQ Advanced Message Security](#)

## Auditování na z/OS

IBM MQ Advanced Message Security for z/OS poskytuje prostředek pro volitelné auditování operací MQI na frontách chráněných zásad. Je-li povolena tato volba, jsou generovány záznamy auditu SMF (System Management Facility) produktu IBM pro úspěch a selhání těchto operací ve frontách chráněných pojistek. Auditované operace zahrnují MQPUT, MQPUT1a MQGET.

Auditování je ve výchozím nastavení vypnuto, můžete aktivovat auditování konfigurací `_AMS_SMF_TYPE` a `_AMS_SMF_AUDIT` v konfigurovaném souboru jazykového prostředí `_CEE_ENVFILE` pro adresní prostor AMS. Další informace naleznete v tématu [Úloha 24: Vytvořit procedury pro rozšířenou bezpečnost zpráv](#). Proměnná `_AMS_SMF_TYPE` se používá k označení typu záznamu SMF a je číslo mezi 128 a 255. Záznam SMF typu 180 je obvykle běžný, avšak není povinný. Auditování je vypnuto uvedením hodnoty 0. Proměnná `_AMS_SMF_AUDIT` konfiguruje, zda jsou vytvořeny záznamy auditu pro operace MQI, které jsou úspěšné, operace MQI, které selžou, nebo obojí. Volby monitorování lze také dynamicky měnit, zatímco AMS je aktivní pomocí příkazů operátora. Další informace najdete v tématu [Provozní prostředí IBM MQ Advanced Message Security](#).

Záznam SMF je definován pomocí podtypů, přičemž podtyp 1 je obecnou událostí auditu. Záznam SMF obsahuje všechna data důležitá pro zpracováváný požadavek.

Záznam SMF je mapován makrem `CSQ0KSMF` (všimněte si nulové hodnoty v názvu makra), který je poskytován v cílové knihovně `SCSQMACS`. Pokud zapisujete programy pro redukci dat pro data SMF, můžete toto makro mapování zahrnout do podpory při vývoji a přizpůsobení rutin následného zpracování SMF.

V záznamech SMF vytvořených produktem IBM MQ Advanced Message Security for z/OS jsou data uspořádána do sekcí. Záznam se skládá z:

- standardní záhlaví SMF
- Rozšíření záhlaví definované parametrem IBM MQ Advanced Message Security pro z/OS
- oddíl produktu
- datová sekce

Sekce produktu záznamu SMF je vždy prezentovaná v záznamech vytvořených produktem IBM MQ Advanced Message Security pro produkt z/OS. Datová sekce se liší v závislosti na podtypu. V současné době je definován jeden podtyp, a proto se používá jedna datová sekce.

Prostředí SMF je popsáno v příručce z/OS System Management Facilities (SA22-7630). Platné typy záznamů jsou popsány v členu `SMFPRMxx` vaší datové sady `PARMLIB`. Další informace naleznete v dokumentaci SMF.

## Generátor sestav auditu IBM MQ Advanced Message Security (CSQ0USMF)

Produkt IBM MQ Advanced Message Security (AMS) for z/OS poskytuje nástroj pro generování sestav auditu s názvem `CSQ0USMF`, který je poskytován v rámci instalace knihovny `SCSQAUTH`. Ukázkový kód JCL ke spuštění obslužného programu `CSQ0USMF` s názvem `CSQ40RSM` je k dispozici v instalační knihovně `SCSQPROC`.

Jako příklad, následující kód JCL vypíše záznamy SMF typu 180 z datové sady SMF a přenesení je do cílové datové sady.

```
//IFAUDUMP EXEC PGM=IFASMFDP
//INDD1 DD DSN=SYSn.MANn.syst,DISP=SHR
//OUTDD1 DD DSN=your.target.dataset,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
INDD(INDD1,OPTIONS(DUMP))
OUTDD(OUTDD1,TYPE(180))
/*
```

Musíte ověřit skutečné názvy datových sad SMF používané vaší instalací. Cílová datová sada pro dumpingové záznamy musí mít formát záznamu VBS a délku záznamu 32760.

**Poznámka:** Pokud se používají proudy protokolů SMF, musíte pomocí programu IFASMF DL vypsat proud protokolu do sekvenční datové sady. Příklad použitých JCL viz [Zpracování typů 116 záznamů SMF](#).

Cílová datová sada pak může být použita jako vstup do obslužného programu CSQ0USMF pro vytvoření sestavy auditu AMS. Příklad:

```
//STEP1 EXEC PGM=CSQ0USMF,
// PARM=('/' -SMFTYPE 180 -M qmgr')
//STEPLIB DD DSN=thlqual.SCSQANLE,DISP=SHR
// DD DSN=thlqual.SCSQAUTH,DISP=SHR
//SMFIN DD DSN=your.target.dataset,DISP=SHR
//
```

Program CSQ0USMF přijímá dva volitelné parametry, které jsou uvedeny v následující tabulce:

Tabulka 84. Volitelné parametry CSQ0USMF		
Parametr	Hodnota	Popis
SMFTYP	nnn	Typ záznamu SMF použitelný pro sestavu auditu. Program CSQ0USMF používá při generování sestavy pouze záznamy SMF, které se shodují s hodnotou SMFTYPE. Pokud neuvédete parametr SMFTYPE, použije se výchozí hodnota 180.
M	QMGR	Název správce front WMQ, který je použitelný pro sestavu auditu. Nezadáte-li parametr -M, bude sestava auditu obsahovat všechny záznamy auditu pro všechny správce front reprezentované v datové sadě SMFIN.

## Používání úložišť klíčů a certifikátů

K zajištění transparentní kryptografické ochrany pro aplikace IBM MQ používá produkt IBM MQ Advanced Message Security soubor úložiště klíčů, kde jsou uloženy certifikáty veřejných klíčů a soukromý klíč. V systému z/OS se místo souboru úložiště klíčů používá svazek klíčů SAF.

V produktu IBM MQ Advanced Message Security jsou 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.

V systémech Windows a UNIX je umístění úložiště klíčů poskytnuto v konfiguračním souboru úložiště klíčů, který je ve výchozím nastavení `keystore.conf`. Každý uživatel produktu IBM MQ Advanced Message Security musí mít konfigurační soubor úložiště klíčů, který ukazuje na soubor úložiště klíčů. IBM MQ Advanced Message Security přijímá následující formát souborů úložiště klíčů: `.kdb`, `.jceks`, `.jks`.

Standardní umístění souboru `keystore.conf` je:

- V systémech SYSTÉM UNIX a IBM i: `$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 -DMQS_KEYSTORE_CONF=path/filename app_name`
  - Pro klienta a server jazyka C:
    - V systému SYSTÉM UNIX a 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

“Rozlišovací jména odesílatelů v AMS” na stránce 489

Rozlišující názvy (DN) odesílatelů identifikují uživatele, kteří mají oprávnění k umístění zpráv do fronty.

“Rozlišující názvy příjemců v produktu AMS” na stránce 490

Rozlišovací jména (DN) příjemců identifikují uživatele, kteří mají oprávnění k načítání zpráv z fronty.

## Struktura konfiguračního souboru úložiště klíčů (keystore.conf) pro AMS

Konfigurační soubor úložiště klíčů (`keystore.conf`) ukazuje Advanced Message Security na umístění příslušného úložiště klíčů.

Každý z následujících typů konfiguračních souborů má předponu:

### cms

Systém správy certifikátů, položky konfigurace mají předponu: `cms`.

### PKCS#11

Standard PKCS (Public Key Cryptography Standard) #11, položky konfigurace mají předponu: `pkcs11`.

### PEM

Formát ochrany soukromí Enhanced Mail, položky konfigurace mají předponu: `pem`.

### JKS

Java KeyStore, položky konfigurace mají předponu: `jks`.

### JCEKS

Java Cryptographic Encryption KeyStore, položky konfigurace mají předponu: `jceks`.

Ukázkové struktury pro úložiště klíčů:

#### cms

```
cms.keystore = /dir/keystore_file
cms.certificate = certificate_label
```

#### PKCS#11

```
pkcs11.library = dir\cryptoki.dll
pkcs11.certificate = certificate_label
pkcs11.token = token_label
pkcs11.token_pin = token_pin
pkcs11.secondary_keystore = dir\signers
```

#### PEM

```
pem.private = /dir/keystore_file_private_key
pem.public = /dir/keystore_file_public_keys
pem.password = password
```

#### Java JKS

```
jks.keystore = dir/Keystore
jks.certificate = certificate_label
jks.encrypted = no
```

```
jks.keystore_pass = password
jks.key_pass = password
jks.provider = IBMJCE
```

## Java JCEKS

```
jceks.keystore = dir/Keystore
jceks.certificate = certificate_label
jceks.encrypted = no
jceks.keystore_pass = password
jceks.key_pass = password
jceks.provider = IBMJCE
```

Tabulka 85. Souhrn parametrů potřebných pro každý typ konfiguračního souboru

Parametry	Typ konfiguračního souboru			
	Java (JKS a JCEKS)	PEM	PKCS#11	cms
keystore	✓			✓
private		✓		
public		✓		
password		✓		
library			✓	
certificate	✓		✓	✓
token			✓	
token_pin			✓	
secondary_keystore			✓	
encrypted	✓			
keystore_pass	✓			
provider	✓			

Parametry konfiguračního souboru jsou definovány následujícím způsobem:

### keystore

Pouze konfigurace CMS a Java . Cesta k souboru úložiště klíčů pro konfiguraci CMS, JKS a JCEKS.

#### Důležité:

- Cesta k souboru úložiště klíčů nesmí obsahovat příponu souboru.

### private

Pouze konfigurace PEM. Název souboru souboru, který obsahuje soukromý klíč a certifikát ve formátu PEM.

### public

Pouze konfigurace PEM. Název souboru souboru, který obsahuje důvěryhodné veřejné certifikáty ve formátu PEM.

### password

Pouze konfigurace PEM. Heslo, které se používá k dešifrování zašifrovaného soukromého klíče.



## library

Pouze PKCS#11 . Jméno cesty ke knihovně PKCS#11 .

## certificate

Pouze konfigurace CMS, PKCS#11 a Java . Popisek certifikátu

## token

Pouze PKCS#11 . Označení tokenu.

## token\_pin

Pouze PKCS#11 . Kód PIN pro odemknutí tokenu.

## secondary\_keystore

Pouze PKCS#11 . Název cesty úložiště klíčů CMS, které je poskytnuto bez rozšíření produktu . kdb , které obsahuje kotvící certifikáty (kořenové certifikáty) vyžadované certifikáty uloženými na tokenu PKCS #11 . Sekundární úložiště klíčů může také obsahovat certifikáty, které jsou intermediační v řetězci trust, stejně jako certifikáty příjemce, které jsou definovány v zásadě zabezpečení ochrany soukromí. Toto úložiště klíčů CMS musí být doprovázeno souborem pro uložení, který musí být umístěn ve stejném adresáři jako sekundární úložiště klíčů.

## encrypted

Pouze konfigurace produktu Java . Stav hesla.

## keystore\_pass

Pouze konfigurace produktu Java . Heslo pro soubor úložiště klíčů.

### Poznámka:

- Pro úložiště klíčů CMS AMS spoléhá na soubory stash ( . sth ), zatímco JKS a JCEKS mohou vyžadovat heslo jak pro certifikát, tak pro soukromý klíč uživatele.
- **Důležité:** Ukládání hesel ve formátu prostého textu je bezpečnostním rizikem.

## key\_pass

Pouze konfigurace produktu Java . Heslo pro soukromý klíč uživatele.

**Důležité:** Ukládání hesel ve formátu prostého textu je bezpečnostním rizikem.

## provider

Pouze konfigurace produktu Java . Poskytovatel zabezpečení produktu Java , který implementuje kryptografické algoritmy vyžadované certifikátem úložiště klíčů.

**Důležité:** Informace, které jsou uloženy v úložišti klíčů, jsou rozhodující pro zabezpečený tok dat, který se odesílá pomocí produktu IBM MQ. Administrátoři zabezpečení musí věnovat zvláštní pozornost, když jim přiřazují oprávnění k souboru těchto souborů.

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 = passwd
jceks.key_pass = passwd
jceks.provider = IBMJCE
```

## Související úlohy

[“Ochrana hesel v produktu Java” na stránce 481](#)

Uložení hesel úložiště klíčů a soukromých klíčů jako prostý text představuje bezpečnostní riziko, takže produkt IBM MQ Advanced Message Security poskytuje nástroj, pomocí kterého lze tato hesla zakódovat pomocí klíče uživatele, který je k dispozici v souboru úložiště klíčů.

Interception MCA umožňuje správci front spuštěnému v rámci produktu IBM MQ selektivně povolit použití zásad pro kanály připojení serveru.

Interception MCA umožňuje klientům, kteří zůstanou mimo produkt IBM MQ Advanced Message Security, stále být připojeni ke správci front, a jejich zprávy budou šifrovány a dešifrovány.

Funkce MCA interception je určen k poskytnutí funkce IBM MQ AMS, pokud IBM MQ AMS nelze povolit na klientovi. Všimněte si, že použití zachycení agenta MCA a klienta s aktivovanou IBM MQ AMS má za následek dvojí ochranu zpráv, které mohou být problematické pro příjem aplikací. Další informace viz [“Zakázání produktu Advanced Message Security na straně klienta”](#) na stránce 471.

## Konfigurační soubor úložiště klíčů

Při výchozím nastavení je konfigurační soubor úložiště klíčů pro zachycení agenta MCA `keystore.conf` a nachází se v adresáři `.mqsc` v cestě k adresáři HOME uživatele, který spustil správce front nebo modul listener. Úložiště klíčů lze také konfigurovat pomocí proměnné prostředí `MQS_KEYSTORE_CONF`. Další informace o konfiguraci úložiště klíčů produktu IBM MQ AMS naleznete v tématu [“Používání úložiště klíčů a certifikátů”](#) na stránce 465.

Chcete-li povolit zachycení agenta MCA, je třeba zadat název kanálu, který chcete použít v konfiguračním souboru úložiště klíčů. Ve specifickém případě typu MCA Interception lze použít pouze typ úložiště klíčů `cms`.

Příklad nastavení zachycení MCA naleznete v tématu [“Příklad příkazu IBM MQ Advanced Message Security MCA interception”](#) na stránce 469.



**Upozornění:** Na vybraných kanálech musíte dokončit ověření a šifrování klienta, například pomocí SSL a SSLPEER nebo CHLAUTH TYPE (SSLPEERMAP), abyste zajistili, že se k této schopnosti budou moci připojit pouze autorizovaní klienti.

Pokud váš podnik používá produkt IBM i a vy jste vybrali komerční certifikační autoritu (CA) k podepsání certifikátu, produkt Digital Certificate Manager vytvoří žádost o certifikát ve formátu PEM (Privacy-Enhanced Mail). Je třeba předat požadavek na zvolenou CA.

Chcete-li to provést, je třeba použít následující příkaz k výběru správného certifikátu pro kanál určený v produktu `channelname`:

```
pem.certificate.channel.<channelname>
```

## Příklad příkazu IBM MQ Advanced Message Security MCA interception

Příklad úlohy, jak nastavit zachycení agenta MCA IBM 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.

Pokud váš podnik používá produkt IBM i a vy jste vybrali komerční certifikační autoritu (CA) k podepsání certifikátu, produkt Digital Certificate Manager vytvoří žádost o certifikát ve formátu PEM (Privacy-Enhanced Mail). Je třeba předat požadavek na zvolenou CA.

### Informace o této úloze

Tato úloha vás provede procesem nastavení vašeho systému tak, aby používal zachycování zpráv MCA, a poté ověření nastavení.

**Poznámka:** Před verzí IBM WebSphere MQ 7.5 byl produkt IBM MQ AMS přidavným produktem, který měl být instalován a zachytávač konfigurován pro ochranu aplikací. Od produktu Verze 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 Verze 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 MQ ochránili.



**Upozornění:** Nahrďte `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/mq80
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 passwd -stash
gsk8capicmd_64 -keydb -create -db $KEYSTORELOC/bobkey.kdb -pw passwd -stash
gsk8capicmd_64 -cert -create -db $KEYSTORELOC/alicekey.kdb -pw passwd
-label alice_cert -dn "cn=alice,O=IBM,c=IN" -default_cert yes
gsk8capicmd_64 -cert -create -db $KEYSTORELOC/bobkey.kdb -pw passwd
-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 7.1 nebo dřívější klient. Vložte následující dvě zprávy:

```
/opt/mqm/samp/bin/amqsputc TESTQ TESTQMGR
```

13. Odeberte zásadu zabezpečení a ověřte výsledek:

```
setmqsp1 -m AMSQMGR1 -p TESTQ -remove  
dspmqsp1 -m AMSQMGR1
```

14. Procházejte frontu z instalace produktu IBM MQ 8.0 :

```
/opt/mq80/samp/bin/amqsbcg TESTQ AMSQMGR1
```

Výstup procházení zobrazuje zprávy v šifrovaném formátu.

15. Nastavte zásadu zabezpečení a ověřte výsledek:

```
setmqsp1 -m AMSQMGR1 -s SHA256 -e AES256 -p TESTQ -a "CN=alice,0=IBM,C=IN"  
-r "CN=alice,0=IBM,C=IN"  
dspmqsp1 -m AMSQMGR1
```

16. Spusťte produkt **amqsgetc** z instalace produktu IBM MQ 8.0 :

```
/opt/mqm/samp/bin/amqsgetc TESTQ TESTQMGR
```

### Související úlohy

[“Stručná úvodní příručka pro IBM MQ AMS s klienty Java” na stránce 453](#)

Pomocí této příručky můžete rychle nakonfigurovat produkt IBM MQ Advanced Message Security a poskytnout zabezpečení zpráv pro aplikace produktu Java , které se připojují pomocí vazeb klienta. Po dokončení tohoto procesu jste vytvořili úložiště klíčů k ověření identit uživatelů a definované zásady pro podepisování a šifrování pro správce front.

### Související odkazy

[“Známá omezení.” na stránce 441](#)

Informace o omezeních produktu IBM MQ Advanced Message Security.

## Zakázání produktu Advanced Message Security na straně klienta

Pokud používáte klienta produktu Verze 7.5 nebo novější pro připojení ke správci front z dřívější verze produktu a je hlášena chyba 2085 (MQRC\_UNKNOWN\_OBJECT\_NAME) , je třeba vypnout produkt IBM MQ Advanced Message Security (AMS).

### Informace o této úloze

V produktu Verze 7.5 je produkt IBM MQ Advanced Message Security (AMS) automaticky aktivován v klientovi IBM MQ a při výchozím nastavení se klient pokusí zkontrolovat zásady zabezpečení pro objekty ve správci front. Nicméně servery ve starších verzích produktu, například Verze 7.1, nemají povoleny AMS a způsobí chybu 2085 (MQRC\_UNKNOWN\_OBJECT\_NAME) chyby.

**V 8.0.0.2** Je-li tato chyba hlášena při pokusu o připojení ke správci front ze starší verze produktu, můžete produkt AMS vypnout následujícím způsobem:

- Pro klienty produktu Java lze následujícími způsoby:
  - Nastavením proměnné prostředí AMQ\_DISABLE\_CLIENT\_AMS.
  - Nastavením systémové vlastnosti Java na hodnotu com.ibm.mq.cfg.AMQ\_DISABLE\_CLIENT\_AMS.
  - Použitím vlastnosti DisableClientAMS, pod stanzou **Security** v souboru mqclient.ini .
- Pro klienty typu C platí jedním z následujících způsobů:
  - Nastavením proměnné prostředí MQS\_DISABLE\_ALL\_INTERCEPT.

- Použitím vlastnosti `DisableClientAMS`, pod stanzou **Security** v souboru `mqclient.ini`.

**Poznámka:** V produktu Verze 7.5 můžete také použít proměnnou prostředí `AMQ_DISABLE_CLIENT_AMS` pro klienty jazyka C. V produktu IBM MQ 8.0 již nelze použít proměnnou prostředí `AMQ_DISABLE_CLIENT_AMS` pro klienty jazyka C. Namísto toho je třeba použít proměnnou prostředí `MQS_DISABLE_ALL_INTERCEPT`.

## Procedura

- Chcete-li v klientu vypnout AMS, použijte jednu z následujících možností:

### proměnná prostředí `AMQ_DISABLE_CLIENT_AMS`

Tuto proměnnou je třeba nastavit v následujících případech:

- Používáte-li prostředí JRE (Java Runtime Environment) jiné než prostředí IBM Java Runtime Environment (JRE)
- Používáte-li produkt Verze 7.5 nebo novější IBM MQ classes for JMS nebo klienta IBM MQ classes for Java.

Vytvořte proměnnou prostředí `AMQ_DISABLE_CLIENT_AMS` a nastavte ji na hodnotu `TRUE` v prostředí, v němž je aplikace spuštěna. Příklad:

```
export AMQ_DISABLE_CLIENT_AMS=TRUE
```

### Vlastnost systému Java `com.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS`

V případě klientů IBM MQ classes for JMS a IBM MQ classes for Java můžete nastavit systémovou vlastnost Java `com.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS` na hodnotu `TRUE` pro aplikaci Java.

Například, můžete nastavit systémovou vlastnost Java jako volbu `-D`, když je vyvolán příkaz Java:

```
java -Dcom.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS=TRUE -cp <MQ_INSTALLATION_PATH>/java/lib/com.ibm.mqjms.jar my.java.applicationClass
```

Případně můžete zadat systémovou vlastnost Java v rámci konfiguračního souboru `JMS jms.config`, pokud aplikace tento soubor používá.

### proměnná prostředí `MQS_DISABLE_ALL_INTERCEPT`

Tuto proměnnou je třeba nastavit v případě, že používáte produkt Verze 8.0 s nativními klienty a u klienta je třeba zakázat produkt AMS.

Vytvořte proměnnou prostředí `MQS_DISABLE_ALL_INTERCEPT` a nastavte ji na hodnotu `TRUE` v prostředí, v němž je klient spuštěn. Příklad:

```
export MQS_DISABLE_ALL_INTERCEPT =TRUE
```

Proměnnou prostředí `MQS_DISABLE_ALL_INTERCEPT` můžete použít pouze pro klienty jazyka C. Pro klienty produktu Java je třeba namísto toho použít proměnnou prostředí `AMQ_DISABLE_CLIENT_AMS`.

### Vlastnost `DisableClientAMS` v souboru `mqclient.ini`

Tuto volbu můžete použít pro klienty IBM MQ classes for JMS a IBM MQ classes for Java a pro klienty C.

Přidejte název vlastnosti `DisableClientAMS` pod stanzou **Security** souboru `mqclient.ini`, jak ukazuje následující příklad:

```
Security:  
DisableClientAMS=Yes
```

Můžete také povolit produkt AMS, jak ukazuje následující příklad:

```
Security:  
DisableClientAMS=No
```

## Jak pokračovat dále

Další informace o problémech s otevíráním chráněných front AMS naleznete v tématu [“Problémy při otevírání chráněných front při použití JMS”](#) na stránce 509.

### Související pojmy

[“Promočování agenta MCA \(Message Channel Agent\)”](#) na stránce 469

Interception MCA umožňuje správci front spuštěnému v rámci produktu IBM MQ selektivně povolit použití zásad pro kanály připojení serveru.

### Související informace

[Konfigurační soubor IBM MQ classes for JMS](#)

[Konfigurace klienta pomocí konfiguračního souboru](#)

## Požadavky na certifikát pro AMS

Certifikáty musí mít veřejný klíč RSA, aby jej bylo možné použít s produktem Advanced Message Security.

Další informace o různých typech veřejných klíčů a o tom, jak je vytvořit, viz [“Digitální certifikáty a kompatibilita CipherSpec v produktu IBM MQ”](#) na stránce 44.

## Rozšíření použití klíče

Rozšíření pro použití klíče umístí další omezení na způsob, jakým lze použít certifikát.

V produktu IBM MQ Advanced Message Security musí 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 492

IBM MQ Advanced Message Security zásady ochrany dat znamenají kvalitu ochrany (QOP).

## Metody ověření platnosti certifikátů v produktu IBM MQ AMS

Pomocí produktu IBM 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 MQ AMS umožňuje ověřit platnost certifikátu pomocí protokolu OCSP (Online Certificate Status Protocol) nebo seznamu odvolaných certifikátů (CRL).

Produkt IBM MQ AMS lze nakonfigurovat buď pro kontrolu OCSP, nebo pro kontrolu CRL, nebo obojí. Jsou-li povoleny obě metody, pak produkt IBM MQ AMS z důvodů výkonu nejprve použije OCSP pro stav odvolání jako první. Pokud je stav odvolání certifikátu neurčený po kontrole OCSP, produkt IBM MQ AMS použije kontrolu CRL.

Všimněte si, že při výchozím nastavení je povolena kontrola OCSP i CRL.

### Související pojmy

[“Protokol OCSP \(Online Certificate Status Protocol\)”](#) na stránce 474

Protokol OCSP (Online Certificate Status Protocol) určuje, zda byl certifikát odvolán, a proto pomáhá určit, zda může být certifikát důvěryhodný. Protokol OCSP je ve výchozím nastavení povolen.

[“Seznamy odvolaných certifikátů \(CRL\)”](#) na stránce 476

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 může být certifikát důvěryhodný. Protokol OCSP je ve výchozím nastavení povolen.

Protokol OCSP není v systémech IBM i systéms podporován.

### Povolení kontroly OCSP pro nativní zachytávače produktu IBM MQ AMS

Kontrola protokolu OCSP (Online Certificate Status Protocol) v produktu IBM MQ Advanced Message Security je standardně povolena na základě informací v použitých certifikátech.

## Postup

Přidejte do konfiguračního souboru úložiště klíčů tyto volby:

**Poznámka:** Všechna stanza OCSP jsou volitelná a lze ji zadat nezávisle.

Volba	Popis
<code>ocsp.enable=off</code>	Povolte kontrolu protokolu OCSP, pokud má kontrolovaný certifikát přístup IIA (Authority Info Access) s přístupovou metodou PKIX_AD_OCSP obsahující identifikátor URI místa, kde se nachází odpovídací modul OCSP. Možné hodnoty: on nebo off.
<code>ocsp.url=&lt; responder_URL &gt;</code>	Adresa URL odpovídacího modulu OCSP. Je-li tato volba vynechána, je kontrola neAIXA protokolu OCSP zakázána.
<code>ocsp.http.proxy.host=&lt; OCSP_proxy &gt;</code>	Adresa URL serveru proxy OCSP. Je-li tato volba vynechána, nebude server proxy použit pro kontroly online certifikátů bez systému AIA.
<code>ocsp.http.proxy.port=&lt; port_number &gt;</code>	Číslo portu serveru proxy OCSP. Je-li tato volba vynechána, bude použit výchozí port 8080.
<code>ocsp.nonce.generation=on/off</code>	Generovat nonce (náhodně generované číslo) při dotazování OCSP. Výchozí hodnota: off.
<code>ocsp.nonce.check=on/off</code>	Kontrolovat nonce (náhodně generované číslo) po přijetí odezvy z OCSP. Výchozí hodnota: off.
<code>ocsp.nonce.size=8</code>	Velikost nonce (náhodně generovaného čísla) v bajtech.
<code>ocsp.http.get=on/off</code>	Určete operaci HTTP GET jako metodu svého požadavku. Je-li pro tuto volbu nastavena hodnota off, použije se metoda HTTP POST. Standardní hodnota je off.
<code>ocsp.max_response_size=20480</code>	Maximální velikost odezvy odpovídacího modulu OCSP v bajtech.
<code>ocsp.cache_size=100</code>	Povolte interní mezipaměť odezvy OCSP a nastavte mezní hodnotu počtu položek mezipaměti.
<code>ocsp.timeout=30</code>	Doba čekání na odezvu serveru v sekundách. Po uplynutí této doby dojde k vypršení časového limitu IBM MQ Advanced Message Security.

Volba	Popis
ocsp.unknown=ACCEPT	Definuje chování, když server OCSP nemůže být dosažen během časového limitu. Možné hodnoty jsou: <ul style="list-style-type: none"> <li>• ACCEPT Povoluje certifikát</li> <li>• WARN Povoluje certifikát a protokoluje varování</li> <li>• REJECT Zabraňuje použití certifikátu a protokoluje chybu</li> </ul>

#### *Povolení kontroly OCSP v produktu Java*

Chcete-li povolit kontrolu OCSP pro produkt Java v produktu IBM MQ Advanced Message Security, upravte soubor `java.security` nebo konfigurační soubor úložiště klíčů.

### Informace o této úloze

V produktu IBM MQ Advanced Message Security lze povolit kontrolu protokolu OCSP dvěma způsoby:

#### *Použití souboru `java.security`*

Zkontrolujte, zda váš certifikát obsahuje rozšíření certifikátu AIA (Authority Information Access).

### Postup

1. Pokud AIA není nastavena nebo chcete přepsat svůj certifikát, upravte soubor `$JAVA_HOME/lib/security/java.security` s následujícími vlastnostmi:

```
ocsp.responderURL=http://url.to.responder:port
ocsp.responderCertSubjectName=CN=Example CA,O=IBM,C=US
```

a umožněte kontrolu OCSP upravením souboru `$JAVA_HOME/lib/security/java.security` následujícím řádkem:

```
ocsp.enable=true
```

2. Je-li nastaveno AIA, povolte kontrolu OCSP upravením souboru `$JAVA_HOME/lib/security/java.security` následujícím řádkem:

```
ocsp.enable=true
```

### Jak pokračovat dále

Pokud používáte správce zabezpečení produktu Java, příliš dokončete konfiguraci, přidejte následující oprávnění produktu Java do produktu `lib/security/java.policy`

```
permission java.security.SecurityPermission "getProperty.ocsp.enable";
```

#### *Použití souboru `keystore.conf`*

### Postup

Přidejte do konfiguračního souboru následující atribut:

```
ocsp.enable=true
```

**Důležité:** Nastavení tohoto atributu v konfiguračním souboru přepíše nastavení `java.security`.



## Jak pokračovat dále

Chcete-li dokončit konfiguraci, přidejte následující oprávnění produktu Java do produktu lib/security/java.policy:

```
permission java.security.SecurityPermission "getProperty.ocsp.enable";
permission java.security.SecurityPermission "setProperty.ocsp.enable";
```

## Seznamy odvolaných certifikátů (CRL)

Seznamy CRL obsahují seznam certifikátů, které byly označeny certifikační autoritou (CA), protože již nejsou důvěryhodné z různých důvodů, například soukromý klíč byl ztracen nebo ohrožen.


Chcete-li ověřit certifikáty, produkt IBM MQ Advanced Message Security vytvoří řetěz certifikátů, který se skládá z certifikátu podepsaného a certifikačního řetězce certifikační autority (CA 's) až po kotvu důvěryhodnosti. Kotva důvěryhodnosti je důvěryhodný soubor úložiště klíčů, který obsahuje důvěryhodný certifikát, nebo důvěryhodný kořenový certifikát, který se používá k deklarování důvěryhodnosti certifikátu. Produkt IBM MQ AMS ověřuje cestu certifikátu pomocí ověřovacího algoritmu PKIX. Když je řetěz vytvořen a ověřen, IBM 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 MQ AMS ověří, zda jsou nastaveny také položky **digitalSignature** nebo **nonRepudiation**. Pokud nejsou, je MQRC\_SECURITY\_ERROR ohlášen a zaprotokolován. Produkt IBM MQ AMS dále stahuje seznamy CRL ze souborů nebo z LDAP v závislosti na tom, jaké hodnoty byly zadány v konfiguračním souboru. IBM MQ AMS podporuje pouze seznamy CRL, které jsou kódovány ve formátu DER. Není-li v konfiguračním souboru úložiště klíčů nalezena žádná konfigurace CRL, IBM MQ AMS neprovede žádnou kontrolu platnosti CRL. Pro každý certifikát CA IBM MQ AMS dotazuje LDAP na CRL pomocí rozlišujících názvů CA pro vyhledání svého seznamu CRL. Do dotazu LDAP jsou zahrnuty následující atributy:

```
certificateRevocationList,
certificateRevocationList;binary,
authorityRevocationList,
authorityRevocationList;binary
deltaRevocationList
deltaRevocationList;binary,
```

**Poznámka:** Produkt deltaRevocationList je podporován pouze v případě, že je určen jako distribuční body.

*Povolení ověření platnosti certifikátu a podpory seznamu odvolaných certifikátů v nativních zachytávacích*  
Je třeba upravit konfigurační soubor úložiště klíčů tak, aby produkt IBM MQ Advanced Message Security mohl stáhnout soubory CLR ze serveru LDAP (Lightweight Directory Access Protocol).

## Informace o této úloze

 Povolení ověření platnosti certifikátu a podpora seznamu odvolaných certifikátů v nativních zachytávacích není podporováno pro produkt IBM MQ Advanced Message Security v systému IBM i.

## Postup

Přidejte do konfiguračního souboru následující volby:

**Poznámka:** Všechna stanza CRL jsou volitelná a mohou být uvedena nezávisle.

Volba	Popis
crl.ldap.host=< host_name >	Název hostitele serveru LDAP.

Volba	Popis
<code>crl.ldap.port=&lt; port_number &gt;</code>	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 IBM MQ AMS Java úspěšně připojí k serveru LDAP, nedojde k pokusu o stažení seznamů CRL ze zbývajících serverů.
<code>crl.cdp=off</code>	Použijte tuto volbu ke kontrole nebo použití rozšíření CRLDistributionPoints v certifikátech.
<code>crl.ldap.version=3</code>	Číslo verze protokolu LDAP. Možné hodnoty: 2 nebo 3.
<code>crl.ldap.user=cn=&lt; username &gt;</code>	Přihlaste se k serveru LDAP. Není-li tato hodnota zadána, musí být atributy CRL v LDAP musejí být čitelné pro celý svět.
<code>crl.ldap.pass=&lt; password &gt;</code>	Heslo pro server LDAP.
<code>crl.ldap.cache_lifetime=0</code>	Životnost mezipaměti LDAP v sekundách. Možné hodnoty: 0-86400.
<code>crl.ldap.cache_size=50</code>	Velikost mezipaměti LDAP. Tuto volbu lze zadat pouze v případě, že je hodnota <code>crl.ldap.cache_lifetime</code> větší než hodnota 0.
<code>crl.http.proxy.host=some.host.com</code>	Port serveru proxy Http pro načtení CRL CDP.
<code>crl.http.proxy.port=8080</code>	Číslo portu serveru proxy HTTP.
<code>crl.http.max_response_size=204800</code>	Maximální velikost seznamu CRL v bajtech, kterou lze načíst ze serveru HTTP, který je přijat sadou GSKit.
<code>crl.http.timeout=30</code>	Doba čekání na odpověď serveru, v sekundách, po které IBM MQ AMS vyprší časový limit.
<code>crl.http.cache_size=0</code>	Velikost mezipaměti HTTP, v bajtech.
<code>crl.unknown=ACCEPT</code>	Definuje chování, pokud nelze v rámci časového limitu dosáhnout serveru CRL. Možné hodnoty jsou: <ul style="list-style-type: none"> <li>• ACCEPT Povoluje certifikát</li> <li>• WARN Povoluje certifikát a protokoluje varování</li> <li>• REJECT Zabraňuje použití certifikátu a protokoluje chybu</li> </ul>

#### *Povolení podpory seznamu odvolaných certifikátů v produktu Java*

Chcete-li v produktu IBM MQ Advanced Message Security povolit podporu CRL, je třeba upravit konfigurační soubor úložiště klíčů tak, aby produkt IBM 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
<code>crl.ldap.host=&lt; host_name &gt;</code>	Název hostitele LDAP.
<code>crl.ldap.port=&lt; port_number &gt;</code>	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 IBM MQ AMS Java úspěšně připojí k serveru LDAP, nedojde k pokusu o stažení seznamů CRL ze zbývajících serverů.  Produkt Java nepoužívá hodnoty <code>crl.ldap.user</code> a <code>crl.ldapworldp.pass</code> . Nepoužívá při připojování k serveru LDAP uživatele a heslo. V důsledku toho musí být atributy CRL v LDAP na světě čitelné.
<code>crl.cdp=on/off</code>	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
<code>com.ibm.security.enableCRLDP</code>	Tato vlastnost má následující hodnoty: <code>true</code> , <code>false</code> .  Je-li při provádění kontroly odvolání certifikátu nastavena hodnota <code>true</code> , jsou seznamy CRL umístěny s použitím adresy URL z rozšíření certifikátu CRL rozšíření certifikátu.  Je-li nastaven na hodnotu <code>false</code> nebo není nastaven, kontrola seznamu CRL pomocí rozšíření distribučních bodů CRL je zakázána.
<code>ibm.security.certpath.ldap.cache.lifetime</code>	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	<p>Tato vlastnost má následující hodnoty: true, false.</p> <p>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.</p> <p>Je-li tento parametr nastaven na hodnotu false nebo není nastaven, nebudou vytvořeny další objekty LDAPCertStore .</p>

#### Povolení seznamů odvolaných certifikátů (CRL) v systému z/OS

Produkt IBM MQ Advanced Message Security podporuje kontrolu seznamu odvolaných certifikátů (CRL) digitálních certifikátů používaných k ochraně datových zpráv.

#### Informace o této úloze

Je-li tato volba povolena, produkt IBM MQ Advanced Message Security potvrdí certifikáty příjemce, když jsou zprávy vloženy do fronty chráněné soukromí, a ověřovat certifikáty odesílatele, když jsou zprávy načítány z chráněné fronty (integrita nebo soukromí). Validace v tomto případě zahrnuje ověření, že příslušné certifikáty nejsou registrovány v příslušném seznamu CRL.

Produkt IBM MQ Advanced Message Security používá služby zabezpečení SSL systému IBM k ověření platnosti certifikátů odesílatele a příjemce. Podrobnou dokumentaci týkající se ověření certifikátu Systému SSL lze nalézt v příručce z/OS Cryptographic Services System Secure Sockets Layer Programming (SC24-5901).

Chcete-li povolit kontrolu CRL, určete umístění konfiguračního souboru CRL prostřednictvím definice CRLFILE DD v kódu JCL spuštěných úloh pro adresní prostor AMS. Ukázkový konfigurační soubor CRL, který lze upravit, je poskytnut v souboru *thlqual.SCSQPROC* (CSQ40CRL). Nastavení povolená v tomto souboru jsou následující:

Tabulka 86. IBM MQ Advanced Message Security Konfigurační proměnné CRL		
Proměnná	Platné hodnoty	Popis
crl.ldap.host[.n]	<i>název hostitele-nebo-název hostitele: port</i>	Ipaddr/název hostitele vašeho serveru LDAP, který hostí seznamy CRL vašich certifikátů vydavatele. Pokud pro váš server LDAP nezádáte číslo portu, použije se číslo portu určené parametrem <i>crl.ldap.port</i> .
crl.ldap.port	<i>port</i>	Číslo portu TCP/IP vašeho serveru LDAP.
crl.ldap.user	<i>uživatel_ldap</i>	Jméno uživatele LDAP, které má být použito pro připojení k serveru LDAP.
crl.ldap.pass	<i>heslo_ldap</i>	Heslo LDAP přidružené k souboru <i>crl.ldap.user</i> .

Můžete zadat více názvů hostitelů a portů serveru LDAP následujícím způsobem:

```
crl ldap.host.1 = hostname -or hostname:port  
crl ldap.host.2 = hostname -or hostname:port  
crl ldap.host.3 = hostname -or hostname:port
```

Můžete zadat až 10 názvů hostitelů. Pokud nezadáte číslo portu pro servery LDAP, použije se číslo portu určené parametrem `crl.ldap.port`. Každý server LDAP musí používat stejnou kombinaci `crl.ldap.user/passwd` pro přístup.

Když je během inicializace adresního prostoru IBM MQ Advanced Message Security určena konfigurace CRLFILE DD a je povolena kontrola CRL, je konfigurace načtena. Není-li parametr CRLFILE DD zadán, nebo je-li konfigurační soubor CRL nedostupný nebo neplatný, je kontrola CRL zakázána.

Produkt IBM MQ AMS provádí kontrolu CRL pomocí služeb ověřování certifikátu SSL systému IBM následujícím způsobem:

Tabulka 87. IBM MQ Advanced Message Security Kontroly CRL		
Operace	Kvalita ochrany	Ověřil certifikát
PUT	Ochrana soukromí	Příjemce (i)
GET	Integrita/soukromí	Odesílatel

Pokud operace zprávy selže při kontrole seznamu CRL, provede příkaz IBM MQ Advanced Message Security následující akce:

Tabulka 88. IBM MQ Advanced Message Security Chování selhání kontroly CRL	
Operace	Selhání kontroly CRL
PUT	Zpráva se nevloží do cílové fronty. Kód dokončení operace MQCC_FAILED a kód příčiny MQRC_SECURITY_ERROR je vrácen do aplikace.
GET	Zpráva se odstraní z cílové fronty a přesune se do fronty chyb ochrany systému. Kód dokončení operace MQCC_FAILED a kód příčiny MQRC_SECURITY_ERROR je vrácen do aplikace.

IBM MQ AMS pro z/OS používá IBM Systémové služby SSL k ověření certifikátů, které zahrnuje CRL a kontrolu důvěryhodnosti. IBM System SSL poskytuje proměnnou prostředí `GSK_CRL_SECURITY_LEVEL` pro střední provoz kontroly CRL. Příklad:

```
GSK_CRL_SECURITY_LEVEL=MEDIUM
```

Tato proměnná je dokumentována v příručce z/OS Cryptographic Services System Secure Sockets Layer Programming. Mezi platná přiřazení patří:

- LOW-Ověření platnosti certifikátu selže, pokud nelze kontaktovat server LDAP.
- MEDIUM-Ověření platnosti certifikátu vyžaduje, aby byl server LDAP stykatelný, ale nevyžaduje definování seznamu CRL.
- HIGH-Ověření platnosti certifikátu vyžaduje, aby byl server LDAP contactable a seznam CRL, který má být definován.

Výchozí hodnota zabezpečení SSL systému IBM je hodnota MEDIUM. Tuto proměnnou můžete nastavit v konfiguračním souboru určeném prostřednictvím definice ENVARS DD v kódu JCL spuštěných úloh pro adresní prostor AMS. Ukázkový konfigurační soubor proměnné prostředí je poskytnut v souboru `thlqual.SCSQPROC (CSQ40ENV)`.

**Poznámka:** Povinností správců je zajistit, aby příslušné služby LDAP byly k dispozici a udržovat záznamy CRL pro příslušné certifikační autority.

## Ochrana hesel v produktu Java

Uložení hesel úložiště klíčů a soukromých klíčů jako prostý text představuje bezpečnostní riziko, takže produkt IBM MQ Advanced Message Security poskytuje nástroj, pomocí kterého lze 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 najdete v tématu [“Používání úložišť klíčů a certifikátů”](#) na stránce 465.

### Příklad

Zde je příklad takového výstupu:

```
#Fri Jul 30 15:20:29 CEST 2010
jceks.key_pass=MMXh997n5Z0r8uRlJmc5qity9MN2CggGBMKCDxdbn1AyPk1vdgTs0LG6X3C1YT7oDzwaqZF10R4t\r\nm
Zsc7JGAx8nqqxLnAucdGn0NWo6xnjZB1n501YGo12k/
PhaQHhFXKMAU9dKg0f8dj0tCA01X4ETe\r\nfY19LBUt2wk87uM7dSs\=
jceks.keystore_pass=0IdeayBnSCfLG4cFuxEVrk6SYyAsdSPpDqgPf16s9s1M04cqZjNbhgjoA2EXonudHZHH+4s2drvQ
\r\nCUvQgu9GuaBMJK2F20jtHJJ1Y4BVeLW2c2okgawo/
W2J1AdUYKkJ0raYTkDouLaTYTQeulyG0xIl\r\niD2si1xUCxhYvvyhbbY\=
jceks.encrypted=yes
```

## Použití certifikátů v systému z/OS

### Informace o této úloze

Produkt IBM MQ Advanced Message Security implementuje dvě úrovně ochrany: integritu a soukromí. S úrovní integrity se zprávy podepisují pomocí soukromého klíče původce (aplikace provádí operaci MQPUT). Integrita poskytuje detekci změny zprávy, ale samotný text zprávy není šifrován.

Při použití úrovně ochrany soukromí není zpráva podepsána pouze, ale je také zašifrována. Tato zpráva je šifrována pomocí symetrického klíče a algoritmu určeného v příslušné zásadě IBM MQ Advanced Message

Security . Samotný symetrický klíč je šifrován s veřejným klíčem každého příjemce (aplikace provádí MQGET). Veřejné klíče jsou přidruženy k certifikátům uloženým v klíčových kruzích.

Je-li zpráva, která je chráněna soukromě, zařazena do fronty přijímající aplikací provádějící příkaz MQGET, musí být tato zpráva dešifrována. Protože byl zašifrován pomocí veřejného klíče příjemce, musí být dešifrován pomocí soukromého klíče příjemce, který se nachází v klíči svazku klíčů.

### **Použití svazků klíčů SAF**

Produkt IBM MQ Advanced Message Security využívá existující služby svazku klíčů SAF k definování a správě certifikátů potřebných pro podepisování a šifrování. Produkty zabezpečení, které jsou funkčně ekvivalentní produktu RACF , lze použít namísto produktu RACF , pokud poskytují stejnou úroveň podpory.

Efektivní využití svazků klíčů může snížit správu potřebnou ke správě certifikátů.

Po vygenerování certifikátu (nebo při importu) musí být tento certifikát připojen ke klíči, který má být přístupný. Stejný certifikát může být připojen k více než jednomu svazku klíčů.

Produkt IBM MQ Advanced Message Security používá dvě sady svazků klíčů. Jedna sada se skládá z klíčových řetězců vlastněných jednotlivými ID uživatele, které pocházejí nebo přijímají zprávy. Každý svazek klíčů obsahuje soukromý klíč přidružený k certifikátu vlastního ID uživatele. Soukromý klíč každého certifikátu se používá k podepisování zpráv pro fronty chráněné integrity nebo ochranou soukromí. Používá se také k dešifrování zpráv z front chráněných soukromí při příjmu zpráv.

Druhá sada je vlastně jediný svazek klíčů přidružený k adresnímu prostoru AMS. Pro integritu nebo ochranu osobních údajů obsahuje řetězec podpisových certifikátů CA potřebných k ověření podpisu a certifikátu pro podepisování zpráv původce zprávy.

Je-li použita ochrana soukromí, tento svazek klíčů také obsahuje certifikáty příjemců zprávy. Veřejné klíče v těchto certifikátech se používají k zašifrování symetrického klíče, který byl použit k zašifrování dat zprávy, když byla zpráva vložena do chráněné fronty. Když jsou tyto zprávy načteny, je soukromý klíč příslušných příjemců použit k dešifrování symetrického klíče, který je poté použit k dešifrování dat zprávy.

Produkt IBM MQ Advanced Message Security používá při hledání certifikátů a soukromých klíčů název svazku klíčů **drq.ams.keyring** . To platí jak pro uživatele, tak pro klíče adresního prostoru AMS.

Pro ilustraci a další vysvětlení certifikátů a svazku klíčů a jejich role v ochraně dat viz [Souhrn operací souvisejících s certifikátem](#).

Soukromý klíč používaný pro podepisování a dešifrování může mít libovolný popisek, ale musí být připojen jako výchozí certifikát.

Digitální certifikáty a svazky klíčů jsou spravovány v produktu RACF primárně pomocí příkazu RACDCERT.

Další informace o certifikátech, jmenovkách a příkazu RACDCERT naleznete v příručkách *z/OS: Security Server RACF Command Language Reference* a *z/OS: Security Server RACF Security Administrator's Guide*.

### **Autorizace přístupu k příkazu RACDCERT**

Oprávnění k použití příkazu RACDCERT je poinstallační úlohou, která měla být dokončena vaším systémovým programátorem produktu z/OS . Tato úloha zahrnuje udělení příslušných oprávnění administrátorovi zabezpečení produktu IBM MQ Advanced Message Security .

Jako souhrn jsou tyto příkazy potřebné k povolení přístupu k příkazu RACF RACDCERT:

```
RDEFINE FACILITY IRR.DIGTCERT.* UACC(NONE)
PERMIT IRR.DIGTCERT.* CLASS(FACILITY) ID( admin ) ACCESS(CONTROL)
SETOPTS RACLIST(FACILITY) REFRESH
```

V tomto příkladě uvádí *admin* ID uživatele vašeho administrátora zabezpečení nebo libovolného uživatele, kterého chcete použít, příkaz RACDCERT.

## Vytvoření certifikátů a klíčových kruhů

This section documents the steps required to create the certificates and key rings necessary for z/OS users of IBM MQ Advanced Message Security, using a RACF Certificate Authority (CA).

Scénář odesílající aplikace a přijímající aplikace se používá k vysvětlení požadovaných kroků.

V následujících příkladech je uživatel user1 původcem zprávy a uživatelem user2 je příjemce. ID uživatele adresního prostoru IBM MQ Advanced Message Security je WMQAMSD.

Všechny příkazy v příkladech, které jsou zde zobrazeny, jsou vydány z volby ISPF 6 administrativním ID uživatele admin.

### Definování certifikátu lokálního vydavatele certifikátů

Používáte-li jako svého CA RACF, musíte vytvořit certifikát certifikační autority, pokud jste tak dosud neučinili. Zobrazený příkaz vytvoří certifikát certifikační autority (nebo podepisujícího subjektu). Tento příklad vytvoří certifikát s názvem AMSCA, který se použije při vytváření následných certifikátů, které budou odrážet identitu uživatelů a aplikací produktu IBM MQ Advanced Message Security.

Tento příkaz lze upravit, konkrétně SUBJECTSDN, aby odrážel strukturu pojmenování a konvence použité při instalaci:

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('AMSCA') O('ibm') C('us'))
KEYUSAGE(CERTSIGN) WITHLABEL('AMSCA')
```

**Poznámka:** Certifikáty podepsané s tímto certifikátem lokálního vydavatele certifikátů ukazují vydavatele CN=AMSCA, O=ibm, C=us, je-li uveden v seznamu s příkazem RACDCERT LIST.

### Vytvoření digitálního certifikátu pomocí soukromého klíče

Pro každého uživatele produktu IBM MQ Advanced Message Security musí být vygenerován digitální certifikát se soukromým klíčem. V uvedeném příkladu jsou příkazy RACDCERT použity ke generování certifikátů pro uživatele user1 a user2, které jsou podepsány pomocí certifikátu lokálního CA identifikovaného štítkem AMSCA.

```
RACDCERT ID(user1) GENCERT SUBJECTSDN(CN('user1') O('ibm') C('us'))
WITHLABEL('user1') SIGNWITH(CERTAUTH LABEL('AMSCA'))
KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)

RACDCERT ID(user2) GENCERT SUBJECTSDN(CN('user2') O('ibm') C('us'))
WITHLABEL('user2') SIGNWITH(CERTAUTH LABEL('AMSCA'))
KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)

RACDCERT ID(user1) ALTER (LABEL('user1')) TRUST
RACDCERT ID(user2) ALTER (LABEL('user2')) TRUST
```

Příkaz RACDCERT ALTER je požadován pro přidání atributu TRUST do certifikátu. Když je certifikát poprvé vytvořen pomocí této procedury, má odlišný platný rozsah dat než podpisový certifikát. V důsledku toho jej produkt RACF označí jako NOTRUST, což znamená, že se certifikát nemá používat. Použijte příkaz RACDCERT ALTER k nastavení atributu TRUST.

Atributy KEYUSAGE HANDSHAKE, DATAENCRYPT a DOCSIGN musí být zadány pro certifikáty používané produktem IBM MQ Advanced Message Security.

Hodnota KEYUSAGE	Sada indikátorů
navázání komunikace	digitalSignature a keyEncipherment
ŠIFROVÁNÍ DAT	dataEncipherment
DOCEDENÍ	nonRepudiation
CERTSIGN	keyCertZnaménko a cRLSign



## Vytvoření svazků klíčů RACF

Zde uvedené příkazy vytvářejí svazek klíčů pro uživatele s definovanými uživateli produktu RACF user1, user2a uživatele úlohy adresního prostoru IBM MQ Advanced Message Security WMQAMSD. Název svazku klíčů je pevně stanoven IBM MQ Advanced Message Security a musí být zakódován, jak je zobrazeno, bez uvozovek. V názvu se rozlišují velká a malá písmena.

```
RACDCERT ID(user1) ADDRING(drq.ams.keyring)
RACDCERT ID(user2) ADDRING(drq.ams.keyring)
RACDCERT ID(WMQAMSD) ADDRING(drq.ams.keyring)
```

## Připojení certifikátů k prstenům klíčů

Připojte certifikáty uživatele a CA k prstenům klíčů:

```
RACDCERT ID(WMQAMSD) CONNECT(CERTAUTH LABEL('AMSCA')
RING(drq.ams.keyring))
RACDCERT ID(user1) CONNECT(ID(user1) LABEL('user1')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
RACDCERT ID(user2) CONNECT(ID(user2) LABEL('user2')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
RACDCERT ID(WMQAMSD) CONNECT(ID(user2) LABEL('user2')
RING(drq.ams.keyring) USAGE(SITE))
```

Certifikát obsahující soukromý klíč použitý k dešifrování musí být připojen k souboru svazku klíčů uživatele jako výchozí certifikát.

Atribut RACDCERT USAGE (SITE) zabraňuje v přístupu k soukromému klíči v klíčovém kruhu, zatímco atribut USAGE RACDCERT (OSOBNÍ) umožňuje použít soukromý klíč, pokud existuje. Certifikát User2 musí být připojen ke svazku klíčů adresního prostoru AMS, protože je zapotřebí jeho veřejného klíče k zašifrování zpráv, které jsou vloženy do fronty. USAGE (SITE) omezuje riziko soukromého klíče uživatele user2.

Certifikát CERTAUTH s označením AMSCA musí být připojen ke svazku klíčů adresního prostoru IBM MQ Advanced Message Security , protože byl použit k podepsání certifikátu uživatele user1, který je původcem zprávy. Používá se k ověření podpisového certifikátu uživatele user1.

## Ověření klíčového řetězce

Klíčový kroužek by se měl objevit tak, jak je zobrazeno zde, po zadání všech příkazů:

```
RACDCERT ID(user1) LISTRING(drq.ams.keyring)
Digital ring information for user USER1:
Ring:
>drq.ams.keyring<:

Certificate Label Name          Cert Owner  USAGE    DEFAULT
-----
user1                          ID(USER1)  PERSONAL YES

RACDCERT ID(user2) LISTRING(drq.ams.keyring)
Digital ring information for user USER2:
Ring:
>drq.ams.keyring<:

Certificate Label Name          Cert Owner  USAGE    DEFAULT
-----
user2                          ID(USER2)  PERSONAL YES

RACDCERT ID(WMQAMSD) LISTRING(drq.ams.keyring)
Digital ring information for user WMQAMSD:
Ring:
>drq.ams.keyring<:

Certificate Label Name          Cert Owner  USAGE    DEFAULT
-----
AMSCA                          CERTAUTH   CERTAUTH NO
user2                          ID(USER2)  SITE     NO
User1                          ID(USER1)  SITE     NO
```

Výpis jednotlivých certifikátů také ukazuje přidružení kruhu.

```
RACDCERT ID(user2) LIST(label('user2'))
Digital certificate information for user USER2:
```

```
***
Label: user2
Certificate ID: 2QfH8Pny9/LzpKKFmfFA
Status: TRUST
Start Date: 2010/05/03 22:59:53
End Date: 2011/05/04 22:59:52
Serial Number:
>15<:
Issuer's Name:
>OU=AMSCA.0=ibm.C=us<:
Subject's Name:
>CN=user2.0=ibm.C=us<:
Key Usage: HANDSHAKE, DATAENCRYPT, DOCSIGN
Private Key Type: Non-ICSF
Private Key Size: 1024
Ring Associations:
Ring Owner: USER2
Ring:
>drq.ams.keyring<:
Ring Owner: WMQAMSD
Ring:
>drq.ams.keyring<:
```

Chcete-li zlepšit výkon, obsah souboru drq.ams.keyring přidružený k adresnímu prostoru AMS je uložen do mezipaměti pro životnost adresního prostoru. Změny na tomto svazku klíčů se nestanou účinnými automaticky. Administrátor může aktualizovat mezipaměť buď:

- Zastavení a restartování správce front.
- Pomocí příkazu z/OS MODIFY:

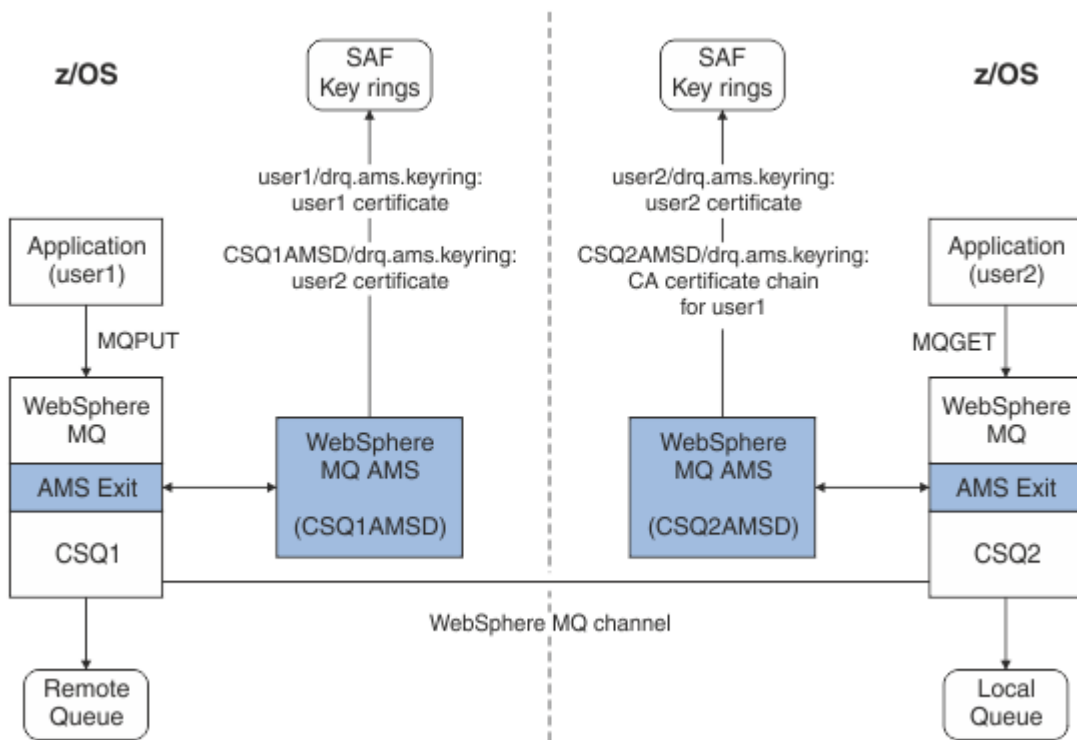
```
F qmgr AMSM,REFRESH KEYRING
```

### **Související informace**

[Provoz IBM MQ Advanced Message Security](#)

### ***Souhrn operací souvisejících s certifikátem***

Obrázek 32 na stránce 486 ilustruje vztahy mezi odesláním a přijímáním aplikací a příslušnými certifikáty. Scénář ilustruje použití vzdálených front mezi dvěma správci front produktu z/OS pomocí zásady ochrany soukromí pro ochranu dat. V produktu [Obrázek 32 na stránce 486](#) označuje "AMS". " IBM MQ Advanced Message Security".



Obrázek 32. Vztahy aplikací a certifikátů

V tomto diagramu aplikace spuštěná jako 'user1' vkládá zprávu do vzdálené fronty spravované správcem front CSQ1, která má být načtena aplikací spuštěnou jako 'user2' z lokální fronty spravované správcem front CSQ2. Diagram předpokládá IBM MQ Advanced Message Security zásadu ochrany soukromí, což znamená, že zpráva je podepsaná i zašifrovaná.

IBM MQ Advanced Message Security zachytává zprávu při vložení a používá certifikát user2 (uložený v souboru svazku klíčů adresního prostoru AMS) k šifrování symetrického klíče použitého k šifrování dat zprávy.

Všimněte si, že certifikát uživatele user2 je připojen k svazku klíčů adresního prostoru AMS s volbou USAGE (SITE). To znamená, že uživatel adresního prostoru AMS má přístup k certifikátu a veřejnému klíči, ale ne k soukromému klíči.

Na přijímajícím konci IBM MQ Advanced Message Security zachycuje vydání user2 a používá certifikát user2 k dešifrování symetrického klíče, aby mohl dešifrovat data zprávy. Poté ověří podpis uživatele user1 pomocí řetězce certifikátu CA uživatele user1 uloženého v klíčovém kruhu uživatele adresního prostoru AMS.

S ohledem na tento scénář, ale s politikou ochrany dat integrity, by certifikáty pro uživatele user2 nebyly požadovány.

Chcete-li použít produkt IBM MQ Advanced Message Security k zařazení zpráv do front chráněných pomocí produktu IBM MQ, které mají zásady ochrany soukromí nebo integrity, IBM MQ Advanced Message Security musí mít přístup k těmto datovým položkám:

- Certifikát X.509 V2 nebo V3 a soukromý klíč pro uživatele zařazování zprávy do fronty.
- Řetěz certifikátů používaný k podepisování digitálních certifikátů všech zpráv podepisujících subjekty.
- Je-li zásada ochrany dat soukromá, jsou příjemci X.509 V2 nebo V3 určeným příjemcům. Zamýšlený příjemci jsou uvedeni v zásadě IBM MQ Advanced Message Security přidružené k frontě.

Pro procesy a aplikace spuštěné v produktu z/OS musí produkt IBM MQ Advanced Message Security obsahovat certifikáty na dvou místech:

- Ve svazku klíčů spravovaného SAF přidružený k identitě RACF odesílající aplikace (aplikace, která zařazuje chráněnou zprávu) nebo přijímající aplikaci (pokud se používá ochrana soukromí).

Certifikát, který produkt IBM MQ Advanced Message Security vyhledá, je výchozím certifikátem a musí obsahovat soukromý klíč. IBM MQ Advanced Message Security předpokládá uživatelskou identitu z/OS odesílající aplikace. To znamená, že se chová jako náhrada, takže má přístup k soukromému klíči uživatele.

- Ve svazku klíčů SAF přidruženém k uživateli adresního prostoru AMS.

Při odesílání zpráv chráněných soukromě tento svazek klíčů obsahuje certifikáty veřejných klíčů příjemců zprávy. Při příjmu zpráv obsahuje řetězec certifikátů certifikačních autorit potřebných k ověření podpisu odesílatele zprávy.

Dřívější příklady použití RACF jako lokálního vydavatele certifikátů (CA). V instalaci však můžete použít jiného poskytovatele PKI (Certificate Authority). Chcete-li použít jiný produkt PKI, nezapomeňte, že soukromý klíč a certifikát musí být importovány do svazku klíčů přidruženého k ID uživatelů produktu z/OS RACF, které pocházejí ze zpráv produktu IBM MQ chráněných produktem IBM MQ Advanced Message Security.

Jako mechanismus pro generování požadavků na certifikáty můžete použít příkaz RACF RACDCERT, který může být exportován a odeslán poskytovateli PKI vaší volby, který má být vydán.

Zde je uveden souhrn kroků souvisejících s certifikátem:

1. Vyžádejte si vytvoření certifikátu CA, v němž RACF je lokální CA. Tento krok vynechte, pokud používáte jiného poskytovatele PKI.
2. Generovat uživatelské certifikáty podepsané CA.
3. Vytvořte svazky klíčů pro uživatele a ID adresního prostoru IBM MQ Advanced Message Security AMS.
4. Připojte certifikát uživatele k souboru svazku klíčů uživatele s výchozím atributem.
5. Připojte certifikáty příjemců do uživatelského svazku klíčů adresního prostoru IBM MQ Advanced Message Security AMS pomocí atributu použití (organizační jednotka) (Tento krok je nezbytný pouze pro uživatelské certifikáty, které budou nakonec příjemci zpráv chráněných soukromě).
6. Připojte řetěz certifikátů CA pro odesílatele zpráv do uživatelského svazku klíčů adresního prostoru IBM MQ Advanced Message Security AMS. (Tento krok je nezbytný pouze pro úlohy AMS, které budou ověřovat podpisy odesílatele.)

### **Konfigurace rezidentní PKI jiného produktu než z/OS**

IBM MQ Advanced Message Security pro z/OS, používá X.509 V3 digitální certifikáty v ochranném zpracování zpráv umístěných nebo přijímaných z front produktu IBM MQ. Produkt IBM MQ Advanced Message Security sám nevytváří ani nespravuje životní cyklus těchto certifikátů; tuto funkci poskytuje infrastruktura veřejných klíčů (PKI). Příklady v této příručce, které ilustrují použití certifikátů, používají server z/OS Security Server RACF k vyplnění žádosti o certifikát.

Je-li použit z/OS nebo není-z/OS používá-li PKI, IBM MQ AMS pro z/OS používá pouze klíčové kruhy, které jsou spravovány RACF nebo jeho ekvivalenty. Tyto svazky klíčů jsou založeny na prostředku SAF (Security Authorization Facility) a jsou úložištěm používaným produktem IBM MQ AMS for z/OS k získání certifikátů pro původce a příjemců zpráv umístěných nebo přijatých z front produktu IBM MQ.

Pro zprávy pocházející z produktu z/OS, které jsou chráněny buď zásadou integrity, nebo zásadou šifrování, musí být certifikát a soukromý klíč původního ID uživatele uloženy ve svazku klíčů spravovaného SAF, který je přidružen k ID uživatele z/OS původce zprávy.

Produkt RACF obsahuje schopnost importovat certifikáty a soukromé klíče do RACF-spravovaných svazků klíčů. Viz publikace z/OS Security Server RACF, kde jsou uvedeny podrobnosti a příklady toho, jak načíst certifikáty do spravovaných klíčů spravovaných klíčů produktu RACF.

Pokud vaše instalace používá jeden z podporovaných produktů PKI, prohlédněte si příručky, které jsou k produktu přiloženy, abyste získali informace o tom, jak ji nasadit.

## Zásady zabezpečení

Produkt IBM 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 MQ Advanced Message Security jsou konceptuální objekty, které popisují způsob, jakým je zpráva šifrovaně šifrována a podepsána.

Podrobnosti o attributech zásad zabezpečení najdete v následujících dílčích tématech:

#### Související pojmy

[“Kvalita ochrany” na stránce 492](#)

IBM MQ Advanced Message Security zásady ochrany dat znamenají kvalitu ochrany (QOP).

[“Atributy zásady zabezpečení” na stránce 491](#)

Můžete použít produkt IBM MQ Advanced Message Security k výběru určitého algoritmu nebo metody k ochraně dat.

#### Název zásady

Název zásady je jedinečný název, který identifikuje specifickou zásadu IBM MQ Advanced Message Security a frontu, na kterou se vztahuje.

Název zásady musí být stejný jako název fronty, na který se vztahuje. Mezi IBM MQ Advanced Message Security ( IBM MQ AMS ) existuje mapování jedna ku jedné. zásady a fronty.

Když vytvoříte zásadu se stejným názvem jako fronta, aktivujete zásadu pro tuto frontu. Fronty bez odpovídajících názvů zásad nejsou chráněny produktem IBM 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 IBM MQ Advanced Message Security šifrované zprávy jsou také podepsány.

**Důležité:** Kvalita ochrany použitá pro funkce vložení a získání zprávy se musí shodovat. Je-li mezi frontou a zprávou ve frontě zjištěna neshoda zásady kvality ochrany, zpráva se neakceptuje a je odeslána do fronty ošetření chyb. Toto pravidlo platí pro lokální i vzdálené fronty.

## Tolerance

Atribut tolerování označuje, zda může produkt IBM MQ Advanced Message Security přijímat zprávy bez uvedené zásady zabezpečení.

Při načítání zprávy z fronty se zásadou pro šifrování zpráv, pokud zpráva není šifrována, je vrácena do volající aplikace. Platné hodnoty:

**0**

Ne (výchozí).

**1**

Ano.

Zásada, která neurčuje hodnotu tolerance nebo má hodnotu 0, znamená, že zprávy umístěné ve frontě přidružené k zásadě musí odpovídat pravidlům zásady.

Tolerance je volitelná a existuje pro usnadnění konfigurace, kdy byly zásady použity ve frontách, ale tyto fronty již obsahují zprávy, které nemají uvedenou zásadu zabezpečení.

## Rozlišovací jména odesílatelů v AMS

Rozlišující názvy (DN) odesílatelů identifikují uživatele, kteří mají oprávnění k umístění zpráv do fronty.

Advanced Message Security (AMS) nekontroluje, zda byla zpráva vložena do fronty s ochranou dat platným uživatelem, dokud se zpráva nenačte. Pokud zásada určuje jednoho či několik platných odesílatelů a uživatel, která zprávu zařadil do fronty, v seznamu platných odesílatelů uveden není, produkt 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) odesílatelů. Pokud pro zásadu nejsou určeny žádné rozlišující názvy odesílatelů, může do fronty zařazovat zprávy s ochranou dat kterýkoli uživatel s důvěryhodným certifikátem.

Tvar rozlišujících názvů odesílatelů 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.
OU	Jednotka v rámci organizace, se kterou je objekt DN přidružen, jako např. obchodní divize nebo název produktu.

Název komponenty	Hodnota
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 odesílatelů, mohou do fronty přidružené k příslušné zásadě zařazovat zprávy pouze tito uživatelé.
- Jsou-li určeny rozlišující názvy odesílatelů, musí přesně odpovídat rozlišujícímu názvu uvedenému v digitálním certifikátu přidruženém k uživateli, který zprávu zařadil.
- 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 UNIX s kódováním UTF-8 zapnutým nebo pomocí grafického uživatelského rozhraní produktu **strmqikm** . Pak musíte vytvořit zásadu z platformy UNIX se zapnutým kódováním UTF-8 nebo použít modul plug-in produktu AMS pro produkt IBM MQ.
- Metoda použitá produktem AMSpro převod názvu odesílatele z formátu x.509 do formátu DN vždy používá hodnotu ST = pro hodnotu Stát nebo Provincie.
- Následující speciální znaky potřebují řídicí znaky:

```
, (comma)
+ (plus)
" (double quote)
\ (backslash)
< (less than)
> (greater than)
; (semicolon)
```

- Pokud rozlišující název obsahuje vložené mezery, uzavřete rozlišující název do dvojitéch uvozovek.

### Související pojmy

“Rozlišující názvy příjemců v produktu AMS” na stránce 490

Rozlišovací jména (DN) příjemců identifikují uživatele, kteří mají oprávnění k načítání zpráv z fronty.

### Rozlišující názvy příjemců v produktu AMS

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.

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).

- 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 tyto uživatelé.
- Jsou-li určeny rozlišující názvy příjemců, musí přesně odpovídat rozlišujícímu názvu uvedenému v digitálním certifikátu přidruženém k uživateli, který zprávu načte.
- 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 UNIX s kódováním UTF-8 zapnutým nebo pomocí grafického uživatelského rozhraní produktu **strmqikm** . Pak musíte vytvořit zásadu z platformy UNIX se zapnutým kódováním UTF-8 nebo použít modul plug-in produktu Advanced Message Security pro produkt IBM MQ.

### Související pojmy

“Rozlišovací jména odesílatelů v AMS” na stránce 489

Rozlišující názvy (DN) odesílatelů identifikují uživatele, kteří mají oprávnění k umísťování zpráv do fronty.

### Atributy zásady zabezpečení

Můžete použít produkt IBM MQ Advanced Message Security k výběru určitého algoritmu nebo metody k ochraně dat.

Zásada zabezpečení je konceptuálním objektem, který popisuje způsob, jakým je zpráva šifrovaně šifrována a podepsána. Následující tabulka uvádí atributy zásad zabezpečení v produktu IBM MQ 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 IBM MQ Advanced Message Security jsou 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 IBM MQ 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***

IBM MQ Advanced Message Security zásady ochrany dat znamenají kvalitu ochrany (QOP).

Tři úrovně ochrany v produktu IBM MQ Advanced Message Security závisejí na šifrovacích algoritmech, které se používají k podepisování a šifrování zprávy:

- Soukromí-zprávy umístěné ve frontě musí být podepsány a šifrovány.
- Integrita-zprávy umístěné ve frontě musí být podepsány odesílatelem.
- 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. Produkt IBM MQ 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:

- V systému SYSTÉM UNIX: <MQInstallRoot>/bin
- Na platformách Windows lze administrativní úlohy spouštět z libovolného umístění, protože proměnná prostředí PATH se aktualizuje při instalaci.
  - V systémech SYSTÉM UNIXa Windows použijete příkazy DELETE POLICY, DISPLAY POLICY a SET POLICY (nebo ekvivalentních PCF) ke správě vašich zásad zabezpečení.
- V systému IBM i jsou příkazy DSPMQMSPL, SETMQMSPL a WRKMQMSPL instalovány do systémové knihovny QSYS pro primární jazyk systému, je-li nainstalován produkt IBM MQ .

Další národní jazykové verze se instalují do knihoven QSYS29xx v závislosti na zavádění jazykových funkcí.

Například počítač s americkou angličtinou jako primární jazyk a korejština jako sekundární jazyk má nainstalované americké anglické příkazy do knihovny QSYS a korejský sekundární jazyk zavedení v QSYS2962 jako 2962 je jazykovým zatížením korejštiny.

- V systému z/OS jsou administrativní příkazy spuštěny pomocí obslužného programu zásad zabezpečení zpráv (CSQOUTIL). Když jsou zásady vytvořeny, upraveny nebo odstraněny na z/OS, změny nejsou rozpoznány produktem IBM MQ Advanced Message Security, dokud není správce front zastaven a restartován, nebo se příkaz z/OS MODIFY použije k aktualizaci konfigurace zásad IBM MQ Advanced Message Security. Příklad:

```
F <qmgr ssid>AMSM,REFRESH POLICY
```

## Související úlohy

[“Vytvoření zásad zabezpečení” na stránce 493](#)

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 494](#)

Pomocí produktu IBM MQ Advanced Message Security můžete změnit podrobnosti o zásadách zabezpečení, které jste již definovali.

[“Zobrazení a výpis zásad zabezpečení” na stránce 495](#)

Příkaz dspmqsp1 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 496](#)

Chcete-li odebrat zásady zabezpečení v produktu IBM MQ Advanced Message Security, je třeba použít příkaz setmqsp1.

## Související informace

[Obslužný program zásad zabezpečení zpráv \(CSQOUTIL\)](#)

[Provoz IBM MQ Advanced Message Security](#)

## 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 pojmenování objektů IBM MQ](#).
- Musíte mít potřebné oprávnění pro připojení ke správci front a vytvořit zásadu zabezpečení. V systému z/OS udělte oprávnění dokumentované v tématu [Obslužný program zásad zabezpečení zpráv \(CSQOUTIL\)](#). Na jiných platformách jiných než z/OS je třeba pomocí příkazu `setmqaut` udělit potřebné oprávnění + connect, + inq a + chg. Další informace o konfiguraci zabezpečení viz [“Nastavení zabezpečení” na stránce 112](#).
- V systému z/OS zajistěte, aby vyžadované systémové objekty byly definovány v souladu s definicemi v souboru CSQ4INSM.

## Příklad

Zde je uveden příklad vytvoření zásady pro správce front QMGR. Zásada určuje, že zprávy mají být podepsány pomocí algoritmu 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:

```
setmqsp1 -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

```
setmqsp1 -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 informace

[Úplný seznam atributů příkazu setmqsp1](#)

## Změna zásad zabezpečení

Pomocí produktu IBM MQ Advanced Message Security můžete změnit podrobnosti o zásadách zabezpečení, které jste již definovali.

## Než začnete

- Správce front, v němž chcete pracovat, musí být spuštěn.
- Musíte mít potřebné oprávnění pro připojení ke správci front a vytvořit zásadu zabezpečení. V systému z/OSudělte oprávnění dokumentované v tématu [Obslužný program zásad zabezpečení zpráv \(CSQOUTIL\)](#). Na jiných platformách jiných než z/OSje třeba pomocí příkazu [setmqaut](#) udělit potřebné oprávnění + connect, + inq a + chg. Další informace o konfiguraci zabezpečení viz [“Nastavení zabezpečení”](#) na stránce 112.

## Informace o této úloze

Chcete-li změnit zásady zabezpečení, použijte příkaz `setmqsp1` 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.

```
setmqsp1 -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 `setmqsp1` 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:

```
setmqsp1 -m QMGR -p MYQUEUE -e AES256 -s SHA1 -a CN=jeff,O=IBM,C=US -r CN=alice,O=IBM,C=US
```

## Související odkazy

[setmqsp1](#)

## 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 potřebné oprávnění pro připojení ke správci front a vytvořit zásadu zabezpečení. V systému z/OS udělte oprávnění dokumentované v tématu [Obslužný program zásad zabezpečení zpráv \(CSQOUTIL\)](#). Na jiných platformách jiných než z/OS je třeba pomocí příkazu `setmqaut` udělit potřebné oprávnění + `connect`, + `inq` a + `chg`. Další informace o konfiguraci zabezpečení viz ["Nastavení zabezpečení"](#) na stránce 112.

### Informace o této úloze

Následuje seznam příznaků příkazu `dspmqspl` :

Tabulka 90. Parametry příkazu <code>dspmqspl</code> .	
Příznak příkazu	Vysvětlení
-m	Název správce front ( <b>povinný</b> ).
-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
```

V systému z/OS je exportovaná informace o zásadě zapsána do souboru CSQOUTIL k příkazu EXPORT DD. Na jiných platformách než z/OS přesměrujte výstup do souboru, například:

```
dspmqspl -m venus.queue.manager -export > policies.[bat|sh]
```

Chcete-li importovat zásady zabezpečení:

- Na platformách Windows spusťte příkaz `policies.bat` .
- V systému SYSTÉM UNIX:
  1. Přihlaste se jako uživatel, který patří do administrativní skupiny produktu mqm IBM MQ .
  2. Zadejte příkaz `. policies.sh`.
- V produktu z/OS použijte obslužný program CSQOUTIL , který uvádí SYSIN datovou sadu obsahující exportované informace o zásadě.

### **Související informace**

Úplný seznam atributů příkazu dspmqspl

### ***Odebrání zásad zabezpečení***

Chcete-li odebrat zásady zabezpečení v produktu IBM MQ Advanced Message Security, je třeba použít příkaz `setmqspl` .

### **Než začnete**

Existují některé vstupní podmínky, které musí být splněny při správě zásad zabezpečení:

- Správce front musí být spuštěn.
- Musíte mít potřebné oprávnění pro připojení ke správci front a vytvořit zásadu zabezpečení. V systému z/OS udělte oprávnění dokumentované v tématu [Obslužný program zásad zabezpečení zpráv \(CSQOUTIL\)](#). Na jiných platformách jiných než z/OS je třeba pomocí příkazu `setmqaut` udělit potřebné oprávnění + `connect`, + `inq` a + `chg`. Další informace o konfiguraci zabezpečení viz [“Nastavení zabezpečení”](#) na stránce 112.

### **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 informace

[Úplný seznam atributů příkazu setmqspl](#)

## Ochrana systémových front

Systémové fronty umožňují komunikaci mezi produktem IBM MQ a jeho pomocnými aplikacemi. Kdykoli je vytvořen správce front, vytvoří se také systémová fronta pro ukládání interních zpráv a dat produktu IBM MQ . Systémové fronty můžete chránit pomocí produktu IBM MQ Advanced Message Security tak, aby k nim mohli přistupovat pouze autorizovaní uživatelé nebo je dešifrovat.

Ochrana systémové fronty se řídí stejným vzorem jako ochrana běžných front. Viz [“Vytvoření zásad zabezpečení”](#) na stránce 493.



Chcete-li použít ochranu systémové fronty na platformách Windows , zkopírujte soubor keystore . conf do následujícího adresáře:











```
c:\Documents and Settings\Default User\.mq\keystore.conf
```

Na jiných platformách než z/OS, které poskytují ochranu 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 k klíčům a certifikátům. Všechny změny provedené v zásadě zabezpečení produktu SYSTEM . ADMIN . COMMAND . QUEUE vyžadují restartování příkazového serveru.

Všechny zprávy odeslané a přijaté z fronty příkazů jsou podepsány nebo podepsány a šifrovány v závislosti na nastavení zásad. Pokud administrátor definuje oprávněné podepisující subjekty, zprávy příkazu, které nepředávají kontrolu rozlišujícího názvu (DN) podepisujícího subjektu, nejsou spuštěny příkazovým serverem a nejsou směrovány do fronty ošetření chyb produktu IBM MQ Advanced Message Security . Zprávy, které jsou odeslány jako odpovědi na dočasné dynamické fronty programu Průzkumník produktu IBM MQ , nejsou chráněny produktem IBM MQ AMS.

Zásady zabezpečení nemají vliv na následující fronty SYSTEM:

- SYSTEM.ADMIN.ACCOUNTING.QUEUE
- SYSTEM.ADMIN.ACTIVITY.QUEUE
- SYSTEM.ADMIN.CHANNEL.EVENT
- SYSTEM.ADMIN.COMMAND.EVENT
-  SYSTEM.ADMIN.COMMAND.QUEUE
- SYSTEM.ADMIN.CONFIG.EVENT
- SYSTEM.ADMIN.LOGGER.EVENT
- SYSTEM.ADMIN.PERFM.EVENT
- SYSTEM.ADMIN.PUBSUB.EVENT
- SYSTEM.ADMIN.QMGR.EVENT
- SYSTEM.ADMIN.STATISTICS.QUEUE
- SYSTEM.ADMIN.TRACE.ROUTE.QUEUE
- SYSTEM.AUTH.DATA.QUEUE
- SYSTEM.BROKER.ADMIN.STREAM
-  SYSTEM.BROKER.CLIENTS.DATA
- SYSTEM.BROKER.CONTROL.QUEUE
- SYSTEM.BROKER.DEFAULT.STREAM

- SYSTEM.BROKER.INTER.BROKER.COMMUNICATIONS
-  SYSTEM.BROKER.SUBSCRIPTIONS.DATA
- SYSTEM.CHANNEL.INITQ
- SYSTEM.CHANNEL.SYNCQ
-  SYSTEM.CHLAUTH.DATA.QUEUE
- SYSTEM.CICS.INITIATION.QUEUE
- SYSTEM.CLUSTER.COMMAND.QUEUE
- SYSTEM.CLUSTER.HISTORY.QUEUE
- SYSTEM.CLUSTER.REPOSITORY.QUEUE
- SYSTEM.CLUSTER.TRANSMIT.QUEUE
-  SYSTEM.COMMAND.INPUT
-  SYSTEM.DDELAY.LOCAL.QUEUE
- SYSTEM.DEAD.LETTER.QUEUE
- SYSTEM.DURABLE.SUBSCRIBER.QUEUE
- SYSTEM.HIERARCHY.STATE
- SYSTEM.INTER.QMGR.CONTROL
- SYSTEM.INTER.QMGR.FANREQ
- SYSTEM.INTER.QMGR.PUBS
- SYSTEM.INTERNAL.REPLY.QUEUE
-  SYSTEM.JMS.PS.STATUS.QUEUE
-  SYSTEM.JMS.REPORT.QUEUE
- SYSTEM.PENDING.DATA.QUEUE
- SYSTEM.PROTECTION.ERROR.QUEUE
- SYSTEM.PROTECTION.POLICY.QUEUE
-  SYSTEM.QSG.CHANNEL.SYNCQ
-  SYSTEM.QSG.TRANSMIT.QUEUE
-  SYSTEM.QSG.UR.RESOLUTION.QUEUE
- SYSTEM.RETAINED.PUB.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 `setmqsp1` a `dspmqsp1`. Produkt IBM MQ Advanced Message Security však spoléhá na správce oprávnění objektu (OAM) a každý pokus o provedení těchto příkazů uživatelem, který nepatří do skupiny `mqm`, která je skupinou administrace produktu IBM MQ, nebo nemá oprávnění číst nastavení zásad zabezpečení, která jsou udělena, a dojde k chybě.

## Postup

Chcete-li uživateli udělit nezbytná oprávnění, spusťte:

```
setmqaut -m SOME.QUEUE.MANAGER -t qmgr -p SOME.USER +connect +inq
setmqaut -m SOME.QUEUE.MANAGER -t queue -n SYSTEM.PROTECTION.POLICY.QUEUE -p SOME.USER +browse
+put
setmqaut -m SOME.QUEUE.MANAGER -t queue -n SYSTEM.PROTECTION.ERROR.QUEUE -p SOME.USER +put
```

**Poznámka:** Tyto oprávnění OAM je třeba nastavit pouze v případě, že máte v úmyslu připojit klienty k správci front pomocí produktu IBM MQ Advanced Message Security Verze 7.0.1.

## Udělení oprávnění zabezpečení

Při použití zabezpečení prostředků příkazu je třeba nastavit oprávnění tak, aby umožňovala funkci produktu IBM MQ Advanced Message Security fungovat. Toto téma používá příkazy RACF v příkladech. Pokud váš podnik používá jiného externího správce zabezpečení (ESM), musíte použít ekvivalentní příkazy pro tento modul ESM.

Pro udělení oprávnění zabezpečení existují tři aspekty:

- [“Adresní prostor AMSM” na stránce 499](#)
- [“CSQOUTIL” na stránce 499](#)
- [“Pomocí front, které mají definovanou zásadu IBM MQ Advanced Message Security .” na stránce 500](#)

**Notes:** Ukázkové příkazy používají následující proměnné.

1. *QMGrName* -Název správce front. V systému z/OS může být tato hodnota také názvem skupiny sdílení front.
2. *username* -Toto může být název skupiny.
3. Příklady zobrazují třídu MQQUEUE. Toto může být také MXQUEUE, GMQQUEUE nebo GMXQUEUE. Další informace viz [“Profily pro zabezpečení fronty” na stránce 185.](#)

Navíc, pokud profil již existuje, nevyžadujete příkaz RDEFINE.

## Adresní prostor AMSM

Je třeba zadat zabezpečení produktu IBM MQ pro jméno uživatele, pod kterým je adresový prostor IBM MQ Advanced Message Security spuštěn.

- Pro dávkové připojení ke správci front zadejte

```
RDEFINE MQCONN QMGrName.BATCH UACC(NONE)
PERMIT QMGrName.BATCH CLASS(MQCONN) ID(username) ACCESS(READ)
```

- Pro přístup k SYSTEM.PROTECTION.POLICY.QUEUE, zadejte:

```
RDEFINE MQQUEUE QMGrName.SYSTEM.PROTECTION.POLICY.QUEUE UACC(NONE)
PERMIT QMGrName.SYSTEM.PROTECTION.POLICY.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(READ)
```

## CSQOUTIL

Obslužný program, který umožňuje uživatelům spouštět příkazy **setmqsp1** a **dspmqsp1**, vyžaduje následující oprávnění, kde jméno uživatele je ID uživatele úlohy:

- Pro dávkové připojení ke správci front zadejte:

```
RDEFINE MQCONN QMGrName.BATCH UACC(NONE)
PERMIT QMGrName.BATCH CLASS(MQCONN) ID(username) ACCESS(READ)
```

- Pro přístup k SYSTEM.PROTECTION.POLICY.QUEUE, vyžadovaná pro příkaz **setmqpol**, vydání:

```
RDEFINE MQQUEUE QMGrName.SYSTEM.PROTECTION.POLICY.QUEUE UACC(NONE)
PERMIT QMGrName.SYSTEM.PROTECTION.POLICY.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(ALTER)
```



- Pro přístup k SYSTEM.PROTECTION.POLICY.QUEUE, vyžadovaná pro příkaz **dspmqp01** , vydání:

```
RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE UACC(NONE)
          PERMIT QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(READ)
```

## Pomocí front, které mají definovanou zásadu IBM MQ Advanced Message Security .

Když aplikace provádí práci s frontami, které mají definovanou zásadu, která má definovanou zásadu, vyžaduje tato aplikace dodatečná oprávnění k tomu, aby produkt IBM MQ Advanced Message Security mohl chránit zprávy.

Aplikace vyžaduje:

- Přístup pro čtení v aplikaci SYSTEM.PROTECTION.POLICY.QUEUE. Postupujte takto:

```
RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE UACC(NONE)
          PERMIT QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(READ)
```

- Přístup k objektu SYSTEM.PROTECTION.ERROR.QUEUE. Postupujte takto:

```
RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.ERROR.QUEUE UACC(NONE)
          PERMIT QMgrName.SYSTEM.PROTECTION.ERROR.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(READ)
```

## IBM i: Nastavení certifikátů a konfiguračního souboru úložiště klíčů

Prvním úkolem při nastavení ochrany produktu IBM MQ Advanced Message Security je vytvoření certifikátu a jeho přidružení k vašemu prostředí. Přidružení je nakonfigurováno prostřednictvím souboru drženého v integrovaném systému souborů (IFS).

### Postup

1. Chcete-li vytvořit certifikát podepsaný držitelem pomocí nástrojů OpenSSL dodávaného s produktem IBM i, zadejte z prostředí QShell tento příkaz:

```
/QOpenSys/usr/bin/openssl req -x509 -newkey rsa:2048 -keyout
$HOME/private.pem -out $HOME/mycert.pem -nodes -days 365
```

Příkaz vás vyzve k zadání různých atributů rozlišujícího názvu pro nový certifikát podepsaný svým držitelem, včetně:

- Běžné jméno (CN =)
- Organizace (O =)
- Země (C =)

Tím se vytvoří nešifrovaný soukromý klíč a odpovídající certifikát, a to jak ve formátu PEM (Privacy Enhanced Mail).

Pro zjednodušení stačí zadat hodnoty pro obecný název, organizaci a zemi. Tyto atributy a hodnoty jsou důležité při vytváření zásady.

2. Produkt IBM MQ AMS vyžaduje, aby jak certifikát, tak soukromý klíč byly uloženy ve stejném souboru. Chcete-li toho dosáhnout, zadejte následující příkaz:

```
cat $HOME/mycert.pem >> $HOME/private.pem
```

Soubor `private.pem` v produktu `$HOME` nyní obsahuje odpovídající soukromý klíč a certifikát, zatímco soubor `mycert.pem` obsahuje všechny veřejné certifikáty, pro které můžete šifrovat zprávy a ověřovat podpisy.

Tyto dva soubory musejí být přidruženy k vašemu prostředí vytvořením konfiguračního souboru úložiště klíčů ( `keystore.conf` ) ve vašem výchozím umístění.

Produkt IBM MQ AMS standardně hledá konfiguraci úložiště klíčů v podadresáři `.mqc` vašeho domovského adresáře.

3. V prostředí QShell vytvořte soubor `keystore.conf` ;

```
mkdir -p $HOME/.mqc
echo "pem.private = $HOME/private.pem" > $HOME/.mqc/keystore.conf
echo "pem.public = $HOME/mycert.pem" >> $HOME/.mqc/keystore.conf
echo "pem.password = unused" >> $HOME/.mqc/keystore.conf
```

## Vytvoření zásady

Před vytvořením zásady je třeba vytvořit frontu, která bude obsahovat chráněné zprávy.

## Postup

1. Na příkazový řádek zadejte příkaz;

```
CRTMQM QNAME(PROTECTED) QTYPE(*LCL) MQMNAME (<mqmname>)
```

kde `mqmname` je název vašeho správce front.

Použijte příkaz `DSPMQM` a zkontrolujte, zda je správce front schopen používat zásady zabezpečení. Ujistěte se, že **Security Policy Capability** zobrazuje `*YES`.

Nejjednodušší zásadou, kterou můžete definovat, je zásada integrity, která je dosažena vytvořením zásady s algoritmem digitálního podpisu, ale bez šifrovacího algoritmu.

Zprávy jsou podepsány, ale nejsou šifrovány. Mají-li být zprávy šifrovány, je třeba určit šifrovací algoritmus a jeden nebo více zamýšlených příjemců zprávy.

Certifikát ve veřejném úložišti klíčů pro požadovaného příjemce zprávy je identifikován pomocí rozlišujícího názvu.

2. Zobrazte rozlišující názvy certifikátů ve veřejném úložišti klíčů, `mycert.pem` v produktu `$HOME`, pomocí následujícího příkazu v prostředí QShell:

```
/QOpenSys/usr/bin/openssl x509 -in $HOME/mycert.pem -noout -subject -nameopt RFC2253
```

Musíte zadat rozlišující název jako požadovaného příjemce a název zásady se musí shodovat s názvem fronty, který má být chráněn.

3. Na příkazovém řádku CL zadejte například:

```
SETMQMSPL POLICY(PROTECTED) MQMNAME (<mqmname>) SIGNALG(*SHA256) ENCALG(*AES256)
RECIPI('CN=.., O=.., C=..')
```

kde `mqmname` je název vašeho správce front.

Jakmile je zásada vytvořena, všechny zprávy, které jsou vhozeny, procházeny nebo destruktivně odebrané přes tento název fronty, jsou předmětem zásady IBM MQ AMS.

## Související informace

[Zobrazení správce front zpráv \(DSPMQM\)](#)

[Nastavení zásady zabezpečení MQM \(SETMQMSPL\)](#)

## Testování zásady

Použijte ukázkové aplikace dodávané spolu s produktem k testování zásad zabezpečení.

## Informace o této úloze

Můžete použít ukázkové aplikace dodávané s produktem IBM MQ , například AMQSPUT4, AMQSGET4, AMQSGBR4a nástroje jako WRKMQMMSG pro vložení, procházení a získání zpráv s použitím názvu fronty PROTECTED.

Za předpokladu, že bylo vše správně nakonfigurováno, nemělo by existovat žádný rozdíl v chování aplikace u nechráněné fronty pro tohoto uživatele.

Uživatel není nastaven pro IBM MQ Advanced Message Security nebo uživatel, který nemá požadovaný soukromý klíč k dešifrování zprávy, však nebude schopen zobrazit zprávu. Uživatel obdrží kód dokončení RCFAIL, který odpovídá MQCC\_FAILED (2) a kód příčiny RC2063 (MQRC\_SECURITY\_ERROR).

Chcete-li vidět, že ochrana AMS je v platnosti, vložte některé testovací zprávy do fronty PROTECTED, například pomocí příkazu AMQSPUT0. Pak můžete vytvořit alias frontu pro procházení nezpracovaných chráněných dat, zatímco ve zbytku.

## Postup

Chcete-li uživateli udělit nezbytná oprávnění, spusťte:

```
CRTMQMQ QNAME(ALIAS) QTYPE(*ALS) TGTQNAME(PROTECTED) MQMNAME(<youmqm>)
```

Procházení s použitím názvu fronty ALIAS, například pomocí příkazu AMQSBCG4 nebo WRKMQMMSG, by mělo odhalit větší počet zpráv produktu scrambled , pokud procházení fronty PROTECTED zobrazuje zprávy cleartext.

Zmašované zprávy jsou viditelné, ale původní prostý text není dešifrován pomocí fronty ALIAS, protože neexistuje žádná zásada pro server AMS, která by vynutila shodu s tímto názvem. Proto jsou vrácena prvotní chráněná data.

### Související informace

[Nastavení zásady zabezpečení MQM \(SETMQMSPL\)](#)

[Práce se zprávami MQ \(WRKMQMMSG\)](#)

## Události příkazů a konfigurace

Pomocí produktu IBM MQ Advanced Message Security můžete generovat zprávy událostí příkazů a konfiguračních událostí, které mohou být protokolovány a sloužit jako záznam změn zásad pro auditování.

Události příkazu a konfigurace generované produktem IBM MQ jsou zprávy o formátu PCF odeslaného do vyhrazených front ve správci front, ve kterém došlo k dané události.

Zprávy událostí konfigurace jsou odeslány na SYSTEM.ADMIN.CONFIG.EVENT .

Zprávy událostí příkazu se odesílají do SYSTEM.ADMIN.COMMAND.EVENT .

Události se generují bez ohledu na nástroje, které používáte ke správě zásad zabezpečení produktu IBM MQ Advanced Message Security .

V produktu IBM MQ Advanced Message Security existují čtyři typy událostí generovaných různými akcemi na zásadách zabezpečení:

- [“Vytvoření zásad zabezpečení” na stránce 493](#), které generují dvě zprávy událostí produktu IBM MQ :
  - Událost konfigurace
  - Událost příkazu
- [“Změna zásad zabezpečení” na stránce 494](#), který generuje tři zprávy událostí produktu IBM MQ :
  - Událost konfigurace, která obsahuje staré hodnoty zásad zabezpečení
  - Událost konfigurace, která obsahuje nové hodnoty zásad zabezpečení
  - Událost příkazu

- “Zobrazení a výpis zásad zabezpečení” na stránce 495, který generuje jednu zprávu události IBM MQ :
  - Událost příkazu
- “Odebrání zásad zabezpečení” na stránce 496, který generuje dvě zprávy událostí produktu IBM 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 informace**

[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 IBM MQ .  
Vráceno: Jako vždycky.

### ***EventQMgr***

Popis: Správce front, ve kterém byl zadán příkaz nebo volání. (Správce front, ve kterém je příkaz spuštěn a který generuje událost, je v MD zprávy události).  
Identifikátor: MQCACF\_EVENT\_Q\_MGR.  
Datový typ: MQCFST.  
Maximální délka: MQ\_Q\_MGR\_NAME\_LENGTH.  
Vráceno: Jako vždycky.

### ***EventAccountingToken***

Popis: Pro příkazy přijaté jako zpráva (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 (AppIdentityData), 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 zpráva (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 IBM MQ 8.0 cmqcfc.h

Vráceno: Jako vždycky.

Příkaz CommandData obsahuje prvky PCF, které obsahují příkaz PCF.

### **Formát zprávy události konfigurace**

Události konfigurace jsou zprávami PCF standardního formátu IBM MQ Advanced Message Security .

Možné hodnoty deskriptoru zpráv MQMD lze nalézt v [Message Message MQMD \(message descriptor\)](#).

Zde jsou vybrané hodnoty MQMD:

```
Format = MQFMT_EVENT
Persistence = MQPER_PERSISTENCE_AS_Q_DEF
PutApplType = MQAT_QMGR //for both CLI and command server
```

Vyrovňovací paměť zpráv se skládá z struktury MQCFH a struktury parametrů, která za ní následuje.

Možné hodnoty MQCFH lze nalézt ve [zprávě události MQCFH \(záhlaví PCF\)](#).

Zde jsou vybrané hodnoty MQCFH:

```
Type = MQCFT_EVENT
Command = MQCMD_CONFIG_EVENT
```

```

MsgSeqNumber = 1 or 2           // 2 will be in case of Change Object event
Control = MQCFC_LAST or MQCFC_NOT_LAST //MQCFC_NOT_LAST will be in case of 1 Change Object
event
ParameterCount = reflects number of PCF parameters following MQCFH
CompCode = MQCC_WARNING
Reason = one of {MQRC_CONFIG_CREATE_OBJECT, MQRC_CONFIG_CHANGE_OBJECT,
MQRC_CONFIG_DELETE_OBJECT}

```

Parametry následující MQCFH jsou:

### **EventUserID**

Popis: ID uživatele, pod kterým byl spuštěn příkaz nebo volání, které událost vygenerovalo. (Toto je stejné ID uživatele, které se používá ke kontrole oprávnění k vydání příkazu nebo volání; pro příkazy přijaté z fronty se jedná také o identifikátor uživatele (UserIdentifier) z MD z příkazové zprávy).

Identifikátor: **MQCACF\_EVENT\_USER\_ID**

Datový typ: MQCFST.

Maximální délka: MQ\_USER\_ID\_LENGTH.

Vráceno: Jako vždycky.

### **SecurityId**

Popis: Hodnota MQMD.AccountingToken v případě zprávy příkazového serveru nebo Windows SID pro lokální příkaz.

Identifikátor: **MQBACF\_EVENT\_SECURITY\_ID**

Datový typ: MQCBS.

Maximální délka: MQ\_SECURITY\_ID\_LENGTH.

Vráceno: Jako vždycky.

### **EventOrigin**

Popis: Původ akce způsobující událost.

Identifikátor: **MQIACF\_EVENT\_IGIN**

Datový typ: MQCFIN.

Hodnoty: **MQEVO\_CONSOLE**  
Příkazový řádek konzoly.  
**MQEVO\_MSG**  
Příkazová zpráva z modulu plug-in průzkumníka produktu IBM MQ .

Vráceno: Jako vždycky.

### **EventQMgr**

Popis: Správce front, ve kterém byl zadán příkaz nebo volání. (Správce front, ve kterém je příkaz spuštěn a který generuje událost, je v MD zprávy události).

Identifikátor: **MQCACF\_EVENT\_Q\_MGR**

Datový typ: MQCFST

Maximální délka: DÉLKA\_MGR\_NÁZVU\_MQ\_QM

Vráceno: Jako vždycky.

### **ObjectType**

Popis:	Typ objektu.
Identifikátor:	<b>MQIACF_OBJECT_TYPE</b>
Datový typ:	MQCFIN
Hodnota:	<b>MQOT_PROTO_POLICY</b> Zásada ochrany IBM MQ Advanced Message Security . <b>1019</b> -Číselná hodnota definovaná v souboru IBM MQ 8.0 nebo v souboru cmqc . h .
Vráceno:	Jako vždycky.

### **PolicyName**

Popis:	Název zásady produktu IBM MQ Advanced Message Security .
Identifikátor:	<b>MQCA_POLICY_NAME.</b>
Datový typ:	MQCFST.
Hodnota:	<b>2112</b> -Číselná hodnota definovaná v souboru IBM MQ 8.0 nebo v souboru cmqc . h .
Maximální délka:	MQ_OBJECT_NAME_LENGTH.
Vráceno:	Jako vždycky.

### **PolicyVersion**

Popis:	Verze zásady produktu IBM MQ Advanced Message Security .
Identifikátor:	<b>MQIA_POLICY_VERSION</b>
Datový typ:	MQCFIN
Hodnota	<b>238</b> -číselná hodnota definovaná v IBM MQ 8.0 nebo v souboru cmqc . h .
Vráceno:	Vždy

### **TolerateFlag**

Popis:	Příznak tolerance zásad IBM MQ Advanced Message Security .
Identifikátor:	<b>Objekt MQIA_TOLEERATE_UNPROTECTED</b>
Datový typ:	MQCFIN
Hodnota	<b>235</b> -číselná hodnota definovaná v IBM MQ 8.0 nebo v souboru cmqc . h .
Vráceno:	Jako vždycky.

### **SignatureAlgorithm**

Popis:	Algoritmus podpisu zásad produktu IBM MQ Advanced Message Security .
Identifikátor:	<b>ALGORITHMUS MQIA_SIGNATURE_ALGORITHM</b>
Datový typ:	MQCFIN
Hodnota:	<b>236</b> -Číselná hodnota definovaná v souboru IBM MQ 8.0 nebo v souboru cmqc . h .
Vráceno:	Kdykoli je definován podpisový algoritmus definovaný v zásadě IBM MQ Advanced Message Security



### **EncryptionAlgorithm**

Popis:	Algoritmus šifrování zásad produktu IBM MQ Advanced Message Security .
Identifikátor:	<b>MQIA_ENCRYPTION_ALGORITHM</b>
Datový typ:	MQCFIN
Hodnota:	<b>237</b> -Číselná hodnota definovaná v souboru IBM MQ 8.0 nebo v souboru cmqc . h .
Vráceno:	Kdykoli je definován šifrovací algoritmus definovaný v zásadě IBM MQ

### **SignerDNs**

Popis:	Předmět DistinguishedName povolených podepisujících subjektů.
Identifikátor:	<b>ROZLIŠUJÍCÍ NÁZEV MQCA_SIGNERDN</b>
Datový typ:	MQCFSL
Hodnota:	<b>2113</b> -Číselná hodnota definovaná v souboru IBM MQ 8.0 nebo v souboru cmqc . h .
Maximální délka:	Nejdelší rozlišující název podepisujícího subjektu v zásadě, ale ne déle než MQ_DISTINGUISHED_NAME_LENGTH
Vráceno:	Kdykoli je definováno v zásadě IBM MQ .

### **RecipientDNs**

Popis:	Předmět DistinguishedName povolených podepisujících subjektů.
Identifikátor:	<b>MQCA_RECIPIENT_DN</b>
Datový typ:	MQCFSL
Hodnota:	<b>2114</b> -Číselná hodnota definovaná v souboru IBM MQ 8.0 nebo v souboru cmqc . h .
Maximální délka:	Nejdelší rozlišující název příjemce v zásadě, ale již není MQ_DISTINGUISHED_NAME_LENGTH.
Vráceno:	Kdykoli je definováno v zásadě IBM MQ .

## **Problémy a řešení**

Jsou poskytnuty informace, které vám pomohou identifikovat a vyřešit problémy související s produktem IBM MQ Advanced Message Security.

V případě problémů souvisejících s produktem IBM MQ Advanced Message Security zkontrolujte nejprve protokol chyb správce front.

### **com.ibm.security.pkcsutil.PKCSException: Chyba šifrování obsahu**

Chyba `com.ibm.security.pkcsutil.PKCSException`: Error encrypting contents naznačuje, že produkt IBM MQ Advanced Message Security má problémy s přístupem k kryptografickým algoritmům.

Pokud příkaz IBM MQ Advanced Message Security vrátí následující chybu:

```
DRQJP0103E The IBM 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 .

Pokud není podpisový algoritmus, který chcete použít, uveden ve vaší aktuální zásadě zabezpečení, stáhněte si správný soubor zásad Java pro vaši verzi produktu z tohoto umístění: [Opravy v produktu IBM Developer Kits](#).

## Podpora OSGi

Chcete-li použít svazek balíků OSGi s dalšími parametry produktu IBM MQ Advanced Message Security , postupujte takto.

Spuštěte 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 MQ AMS podporuje komunikaci pouze s použitím tříd produktu MQ Base Java 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 MQ Advanced Message Security.

Spuštete JMS a obdržíte chybu 2085 (MQRC\_UNKNOWN\_OBJECT\_NAME) spolu s chybou JMSMQ2008.

Ověřili jste, že jste nastavili IBM MQ AMS , jak je popsáno v [“Stručná úvodní příručka pro IBM MQ AMS s klienty Java”](#) na stránce 453.

Možnou příčinou je to, že používáte prostředí JRE (non-IBM Java Runtime Environment). Jedná se o známé omezení popsané v [“Známá omezení.”](#) na stránce 441.

Nenastavili jste proměnnou prostředí AMQ\_DISABLE\_CLIENT\_AMS.

## Řešení problému

Pro práci s tímto problémem jsou k dispozici čtyři možnosti:

1. Spuštěte 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 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 mechanismus 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 MQ AMS.

Další informace viz [“Promočování agenta MCA \(Message Channel Agent\)”](#) na stránce 469.

**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`.

## Příklady konfigurací v systému z/OS

Tato část obsahuje vzorové konfigurace zásad a certifikátů pro IBM MQ Advanced Message Security scénáře řazení do fronty v produktu z/OS.

Příklady zahrnují požadované zásady produktu IBM MQ Advanced Message Security a digitální certifikáty, které musí existovat vzhledem k uživatelům a klíčům klíčů. Příklady předpokládají, že uživatelé, kteří se podíleli na scénářích, byli nastavenými podle pokynů uvedených v části [Úloha 27: Udělit uživatelům oprávnění k prostředkům pro produkt IBM MQ Advanced Message Security](#).

## Lokální ukládání zpráv chráněných heslem do fronty v systému z/OS

Tento příklad podrobně popisuje zásady a certifikáty produktu IBM MQ Advanced Message Security potřebné k odesílání a načítání zpráv chráněných integritou do fronty a z fronty, která je lokální vzhledem k ukládání a získávání aplikací.

Ukázkový správce front a fronta jsou:

```
BNK6      - Queue manager
FIN.XFER.Q7 - Local queue
```

Tito uživatelé se používají:

```
WMQBNK6 - IBM MQ AMS task user
TELLER5 - Sending user
FINADM2 - Recipient user
```

## Vytvoření uživatelských certifikátů

V tomto příkladu je potřeba pouze jeden uživatelský certifikát. Jedná se o certifikát pro odeslání uživatele, který je nutný pro podepisování zpráv chráněných integritou. Odesílající uživatel je 'TELLER5'.

Je také požadován certifikát vydavatele certifikátů (CA). Certifikát CA je certifikát autority, která vydala certifikát uživatele. Může se jednat o řetězec certifikátů. Je-li tomu tak, všechny certifikáty v řetězci jsou vyžadovány v svazku klíčů uživatele úlohy IBM MQ Advanced Message Security, v tomto případě uživatele WMQBNK6.

Certifikát CA lze vytvořit pomocí příkazu RACDCERT produktu RACF. Tento certifikát se používá k vydávání uživatelských certifikátů. Příklad:

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('BCOCA') O('BCO') C('US'))
KEYUSAGE(CERTSIGN) WITHLABEL('BCOCA')
```

Tento příkaz RACDCERT vytvoří certifikát CA, který pak může být použit k vydání uživatelského certifikátu pro uživatele 'TELLER5'. Příklad:

```
RACDCERT ID(TELLER5) GENCERT SUBJECTSDN(CN('Teller5') O('BCO') C('US'))
WITHLABEL('Teller5') SIGNWITH(CERTAUTH LABEL('BCOCA'))
KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)
```

Vaše instalace bude mít procedury pro výběr nebo vytvoření certifikátu CA, stejně jako procedury pro vydávání certifikátů a distribuci těchto certifikátů do příslušných systémů.

Při exportu a importu těchto certifikátů produkt IBM MQ Advanced Message Security vyžaduje:

- Certifikát CA (řetězec).

- Certifikát uživatele a jeho soukromý klíč.

Používáte-li produkt RACF, lze příkaz RACDCERT EXPORT použít k exportování certifikátů do datové sady a příkaz RACDCERT ADD lze použít k importování certifikátů z datové sady. Další informace o těchto a dalších příkazech RACDCERT naleznete v příručce *z/OS: Security Server RACF Command Language Reference*.

Certifikáty v tomto případě jsou vyžadovány na systému z/OS se spuštěným správcem front BNK6.

Pokud byly certifikáty importovány do systému z/OS se systémem BNK6, je tento certifikát uživatele vyžadován atributem TRUST. Příkaz RACDCERT ALTER lze použít k přidání atributu TRUST do certifikátu. Příklad:

```
RACDCERT ID(TELLER5) ALTER (LABEL('Te11er5')) TRUST
```

V tomto příkladu není pro uživatele příjemce požadován žádný certifikát.

## Připojení certifikátů k příslušným klíčovým sdružením

Pokud byly požadované certifikáty vytvořeny nebo importovány a nastaveny jako důvěryhodné, musí být připojeny k příslušným prstenům klíčů uživatele na systému z/OS, kde je spuštěna BNK6. Chcete-li vytvořit svazky klíčů, použijte příkazy RACDCERT ADDRING:

```
RACDCERT ID(WMQBNK6) ADDRING(drq.ams.keyring)
RACDCERT ID(TELLER5) ADDRING(drq.ams.keyring)
```

Tím se vytvoří svazek klíčů pro uživatele úlohy IBM MQ Advanced Message Security, WMQBNK6a svazek klíčů pro odesílající uživatele, 'TELLER5'. Mějte na zřeteli, že název svazku klíčů drq.ams.keyring je povinný a název rozlišuje velká a malá písmena.

Když byly vytvořeny svazky klíčů, mohou být příslušné certifikáty připojeny:

```
RACDCERT ID(WMQBNK6) CONNECT(CERTAUTH LABEL('BCOCA')
RING(drq.ams.keyring))
RACDCERT ID(TELLER5) CONNECT(ID(TELLER5) LABEL('Te11er5')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
```

Odesílající se certifikát uživatele musí být připojen jako VÝCHOZÍ. Pokud má odesílající uživatel více než jeden certifikát ve svém souboru drq.ams.keyring, použije se výchozí certifikát pro účely podepisování.

Vytvoření a úprava certifikátů nejsou produktem IBM MQ Advanced Message Security rozpoznány, dokud není správce front zastaven a restartován, nebo se příkaz z/OS **MODIFY** používá k aktualizaci konfigurace certifikátu produktu IBM MQ Advanced Message Security. Příklad:

```
F BNK6AMSM,REFRESH KEYRING
```

## Vytvoření zásady produktu IBM MQ Advanced Message Security

V tomto příkladu jsou zprávy chráněné integrity vloženy do fronty FIN.XFER.Q7 z aplikace spuštěné jako uživatel 'TELLER5' a načtené ze stejné fronty aplikací spuštěnými jako uživatel 'FINADM2', takže je vyžadována pouze jedna zásada IBM MQ Advanced Message Security.

Zásady produktu IBM MQ Advanced Message Security se vytvářejí pomocí obslužného programu CSQOUTIL, který je zdokumentován v tématu [Obslužný program zásad zabezpečení zpráv \(CSQOUTIL\)](#).

Obslužný program CSQOUTIL použijte ke spuštění následujícího příkazu:

```
setmqsp1 -m BNK6 -p FIN.XFER.Q7 -s MD5 -a CN=Te11er5,0=BCO,C=US
```

V této zásadě je správce front identifikován jako BNK6. Název zásady a přidružená fronta je FIN.XFER.Q7. Algoritmus použitý ke generování podpisu odesílatele je MD5a rozlišující název (DN) odesílajícího uživatele je 'CN=Teller5,O=BCO,C=US'.

Po definování zásady buď restartujte správce front BNK6 , nebo aktualizujte konfiguraci zásad produktu IBM MQ Advanced Message Security pomocí příkazu z/OS **MODIFY** . Příklad:

```
F BNK6AMSM,REFRESH POLICY
```

## Lokální ukládání zpráv chráněných soukromí do fronty v systému z/OS

Tento příklad podrobně popisuje zásady a certifikáty produktu IBM MQ Advanced Message Security potřebné k odesílání a načítání zpráv chráněných soukromě do fronty a z fronty, která je lokální vzhledem k ukládání a získávání aplikací. Zprávy chráněné heslem jsou podepsané i šifrované.

Ukázkový správce front a lokální fronta jsou následující:

```
BNK6          - Queue manager
FIN.XFER.Q8   - Local queue
```

Tito uživatelé se používají:

```
WMQBNK6      - IBM MQ AMS task user
TELLER5      - Sending user
FINADM2      - Recipient user
```

Postup konfigurace tohoto scénáře:

## Vytvoření uživatelských certifikátů

V tomto příkladu se požadují dva uživatelské certifikáty. Jedná se o odesílaný uživatelský certifikát, který je nutný pro podepisování zpráv, a certifikát uživatele příjemce, který je potřebný pro šifrování a dešifrování dat zprávy. Odesílající uživatel je 'TELLER5' a uživatel příjemce je 'FINADM2'.

Je také požadován certifikát vydavatele certifikátů (CA). Certifikát CA je certifikát autority, která vydala certifikát uživatele. Může se jednat o řetězec certifikátů. Je-li tomu tak, všechny certifikáty v řetězci jsou vyžadovány v svazku klíčů uživatele úlohy IBM MQ Advanced Message Security , v tomto případě uživatele WMQBNK6.

Certifikát CA lze vytvořit pomocí příkazu RACDCERT produktu RACF . Tento certifikát se používá k vydávání uživatelských certifikátů. Příklad:

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('BCOCA') O('BCO') C('US'))
KEYUSAGE(CERTSIGN) WITHLABEL('BCOCA')
```

Tento příkaz RACDCERT vytvoří certifikát CA, který pak může být použit k vydávání uživatelských certifikátů pro uživatele 'TELLER5' a 'FINADM2'. Příklad:

```
RACDCERT ID(TELLER5) GENCERT SUBJECTSDN(CN('Teller5') O('BCO') C('US'))
WITHLABEL('Teller5') SIGNWITH(CERTAUTH LABEL('BCOCA'))
KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)

RACDCERT ID(FINADM2) GENCERT SUBJECTSDN(CN('FinAdm2') O('BCO') C('US'))
WITHLABEL('FinAdm2') SIGNWITH(CERTAUTH LABEL('BCOCA'))
KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)
```

Vaše instalace bude mít procedury pro výběr nebo vytvoření certifikátu CA, stejně jako procedury pro vydávání certifikátů a distribuci těchto certifikátů do příslušných systémů.

Při exportu a importu těchto certifikátů produkt IBM MQ Advanced Message Security vyžaduje:

- Certifikát CA (řetězec).
- Odesílající uživatelský certifikát a jeho soukromý klíč.
- Certifikát uživatele příjemce a jeho soukromý klíč.

Používáte-li produkt RACF, lze příkaz RACDCERT EXPORT použít k exportování certifikátů do datové sady a příkaz RACDCERT ADD lze použít k importování certifikátů z datové sady. Další informace o těchto a dalších příkazech RACDCERT naleznete v příručce *z/OS: Security Server RACF Command Language Reference*.

Certifikáty v tomto případě jsou vyžadovány na systému z/OS se spuštěným správcem front BNK6.

Pokud byly certifikáty importovány do systému z/OS se systémem BNK6, uživatelské certifikáty vyžadují atribut TRUST. Příkaz RACDCERT ALTER lze použít k přidání atributu TRUST do certifikátu. Příklad:

```
RACDCERT ID(TELLER5) ALTER (LABEL('Teller5')) TRUST
RACDCERT ID(FINADM2) ALTER (LABEL('FinAdm2')) TRUST
```

## Připojení certifikátů k příslušným klíčovým sdružením

Pokud byly požadované certifikáty vytvořeny nebo importovány a nastaveny jako důvěryhodné, musí být připojeny k příslušným prstenům klíčů uživatele na systému z/OS, kde je spuštěna BNK6. Chcete-li vytvořit svazky klíčů, použijte příkaz RACDCERT ADDRING:

```
RACDCERT ID(WMQBNK6) ADDRING(drq.ams.keyring)
RACDCERT ID(TELLER5) ADDRING(drq.ams.keyring)
RACDCERT ID(FINADM2) ADDRING(drq.ams.keyring)
```

Tím se vytvoří svazek klíčů pro uživatele úlohy IBM MQ Advanced Message Security a svazek klíčů pro odesílající a přijímající uživatele. Mějte na zřeteli, že název svazku klíčů drq.ams.keyring je povinný a název rozlišuje velká a malá písmena.

Když byly vytvořeny svazky klíčů, mohou být příslušné certifikáty připojeny.

```
RACDCERT ID(WMQBNK6) CONNECT(CERTAUTH LABEL('BCOCA')
RING(drq.ams.keyring))

RACDCERT ID(WMQBNK6) CONNECT(ID(FINADM2) LABEL('FinAdm2')
RING(drq.ams.keyring) USAGE(SITE))

RACDCERT ID(TELLER5) CONNECT(ID(TELLER5) LABEL('Teller5')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))

RACDCERT ID(FINADM2) CONNECT(ID(FINADM2) LABEL('FinAdm2')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
```

Odesílající a přijímající uživatelské certifikáty musí být připojeny jako DEFAULT. Má-li uživatel více než jeden certifikát ve svém souboru drq.ams.keyring, použije se výchozí certifikát pro podepisování a pro účely dešifrování.

Certifikát uživatele příjemce musí být také připojen ke klíčovému okruhu uživatele úlohy IBM MQ Advanced Message Security s USAGE (SITE). Důvodem je to, že úloha zabezpečení rozšířených zpráv potřebuje veřejný klíč příjemce při šifrování dat zprávy. USAGE (SITE) zabraňuje tomu, aby byl soukromý klíč přístupný v klíčovému kruhu.

Vytvoření a úprava certifikátů nejsou produktem IBM MQ Advanced Message Security rozpoznány, dokud není správce front zastaven a restartován, nebo se příkaz z/OS **MODIFY** používá k aktualizaci konfigurace certifikátu produktu IBM MQ Advanced Message Security. Příklad:

```
F BNK6AMSM,REFRESH KEYRING
```

## Vytvoření zásady produktu IBM MQ Advanced Message Security

V tomto příkladu jsou zprávy chráněné soukromě vloženy do fronty FIN.XFER.Q8 z aplikace spuštěné jako uživatel 'TELLER5' a načtené ze stejné fronty aplikací spuštěnými jako uživatel 'FINADM2', takže je vyžadována pouze jedna zásada IBM MQ Advanced Message Security .

Zásady produktu IBM MQ Advanced Message Security se vytvářejí pomocí obslužného programu CSQOUTIL , který je zdokumentován v tématu [Obslužný program zásad zabezpečení zpráv \(CSQOUTIL\)](#).

Obslužný program CSQOUTIL použijte ke spuštění následujícího příkazu:

```
setmqsp1 -m BNK6 -p FIN.XFER.Q8 -s SHA1 -e 3DES -a CN=Teller5,O=BCO,C=US -r  
CN=FinAdm2,O=BCO,C=US
```

V této zásadě je správce front identifikován jako BNK6. Název zásady a přidružená fronta je FIN.XFER.Q8. Algoritmus použitý ke generování podpisu odesílatele je SHA1a rozlišující název (DN) odesílajícího uživatele je 'CN=Teller5,O=BCO,C=US' a uživatel příjemce je 'CN=FinAdm2,O=BCO,C=US'. Algoritmus, který se používá k šifrování dat zprávy, je 3DES.

Po definování zásady buď restartujte správce front BNK6 , nebo aktualizujte konfiguraci zásad produktu IBM MQ Advanced Message Security pomocí příkazu z/OS **MODIFY** . Příklad:

```
F BNK6AMSM,REFRESH POLICY
```

## Vzdálené ukládání zpráv chráněných heslem do fronty v systému z/OS

Tento příklad podrobně popisuje zásady a certifikáty produktu IBM MQ Advanced Message Security potřebné k odesílání a načítání zpráv chráněných integritou a z front spravovaných dvěma různými správci front. Dva správci front mohou být spuštěni ve stejném systému z/OS nebo v různých systémech z/OS , nebo jeden správce front může být na distribuovaném systému, na kterém běží IBM MQ Advanced Message Security.

Příklad správců front a front jsou:

```
BNK6      - Sending queue manager  
BNK7      - Recipient queue manager  
FIN.XFER.Q7 - Remote queue on BNK6  
FIN.RCPT.Q7 - Local queue on BNK7
```

Poznámka: V tomto příkladu jsou BNK6 a BNK7 správci front spuštěni na různých systémech z/OS .

Tito uživatelé se používají:

```
WMQBANK6 - IBM MQ AMS task user on BNK6  
WMQBANK7 - IBM MQ AMS task user on BNK7  
TELLER5  - Sending user on BNK6  
FINADM2  - Recipient user on BNK7
```

Postup konfigurace tohoto scénáře je následující:

## Vytvoření uživatelských certifikátů

V tomto příkladu je potřeba pouze jeden uživatelský certifikát. Jedná se o certifikát pro odeslání uživatele, který je nutný k podpisu zprávy chráněné integritou. Odesílající uživatel je 'TELLER5'.

Je také požadován certifikát vydavatele certifikátů (CA). Certifikát CA je certifikát autority, která vydala certifikát uživatele. Může se jednat o řetězec certifikátů. Je-li tomu tak, všechny certifikáty v řetězci jsou vyžadovány v svazku klíčů uživatele úlohy IBM MQ Advanced Message Security , v tomto případě uživatele WMQBANK7.

Certifikát CA lze vytvořit pomocí příkazu RACDCERT produktu RACF . Tento certifikát se používá k vydávání uživatelských certifikátů. Příklad:

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('BCOCA') O('BCO') C('US'))
KEYUSAGE(CERTSIGN) WITHLABEL('BCOCA')
```

Tento příkaz RACDCERT vytvoří certifikát CA, který pak může být použit k vydání uživatelského certifikátu pro uživatele 'TELLER5'. Příklad:

```
RACDCERT ID(TELLER5) GENCERT SUBJECTSDN(CN('Teller5') O('BCO') C('US'))
WITHLABEL('Teller5') SIGNWITH(CERTAUTH LABEL('BCOCA'))
KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)
```

Vaše instalace bude mít procedury pro výběr nebo vytvoření certifikátu CA, stejně jako procedury pro vydávání certifikátů a distribuci těchto certifikátů do příslušných systémů.

Při exportu a importu těchto certifikátů produkt IBM MQ Advanced Message Security vyžaduje:

- Certifikát CA (řetězec).
- Odesílající uživatelský certifikát a jeho soukromý klíč.

Používáte-li produkt RACF, lze příkaz RACDCERT EXPORT použít k exportování certifikátů do datové sady a příkaz RACDCERT ADD lze použít k importování certifikátů z datové sady. Další informace o těchto a dalších příkazech RACDCERT naleznete v příručce *z/OS: Security Server RACF Command Language Reference*.

Certifikáty v tomto případě jsou vyžadovány na systému z/OS se spuštěným správcem front BNK6 a BNK7.

V tomto příkladu musí být odesílající certifikát importován na systému z/OS se systémem BNK6a certifikát CA musí být importován na systému z/OS spouštějícím BNK7. Když certifikáty byly importovány, uživatelský certifikát vyžaduje atribut TRUST. Příkaz RACDCERT ALTER lze použít k přidání atributu TRUST do certifikátu. Například na BNK6:

```
RACDCERT ID(TELLER5) ALTER (LABEL('Teller5')) TRUST
```

## Připojení certifikátů k příslušným klíčovým sdružením

Pokud byly požadované certifikáty vytvořeny nebo importovány a nastaveny jako důvěryhodné, musí být připojeny k příslušným prstenům klíčů uživatele na systému z/OS s operačním systémem BNK6 a BNK7.

Chcete-li vytvořit svazky klíčů, použijte příkaz RACDCERT ADDRING na BNK6:

```
RACDCERT ID(TELLER5) ADDRING(drq.ams.keyring)
```

Tím se vytvoří svazek klíčů pro odeslání uživatele na BNK6. Mějte na zřeteli, že název svazku klíčů drq.ams.keyring je povinný a název rozlišuje velká a malá písmena.

V BNK7:

```
RACDCERT ID(WMQBNK7) ADDRING(drq.ams.keyring)
```

Tím se vytvoří klíčový kroužek pro uživatele úlohy IBM MQ Advanced Message Security na BNK7. Pro 'TELLER5' na BNK7 není požadován žádný svazek klíčů uživatele.

Když byly vytvořeny svazky klíčů, mohou být příslušné certifikáty připojeny.



Dne BNK6:

```
RACDCERT ID(TELLER5) CONNECT(ID(TELLER5) LABEL('Teller5')  
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
```

V BNK7:

```
RACDCERT ID(WMQBNK7) CONNECT(CERTAUTH LABEL('BCOCA')  
RING(drq.ams.keyring))
```

Odesílající se certifikát uživatele musí být připojen jako VÝCHOZÍ. Pokud má odesílající uživatel více než jeden certifikát ve svém souboru drq.ams.keyring, použije se výchozí certifikát pro účely podepisování.

Vytvoření a úprava certifikátů nejsou produktem IBM MQ Advanced Message Security rozpoznány, dokud není správce front zastaven a restartován, nebo se příkaz z/OS **MODIFY** používá k aktualizaci konfigurace certifikátu produktu IBM MQ Advanced Message Security . Příklad:

Dne BNK6:

```
F BNK6AMSM, REFRESH, KEYRING
```

V BNK7:

```
F BNK7AMSM, REFRESH, KEYRING
```

## Vytvoření zásad produktu IBM MQ Advanced Message Security

V tomto příkladu jsou zprávy chráněné integrity vloženy do vzdálené fronty FIN.XFER.Q7 na BNK6 aplikací spuštěnou jako uživatel 'TELLER5' a načtené z lokální fronty FIN.RCPT.Q7 na BNK7 aplikací spuštěnou jako uživatel 'FINADM2', takže jsou vyžadovány dvě zásady IBM MQ Advanced Message Security .

Zásady produktu IBM MQ Advanced Message Security se vytvářejí pomocí obslužného programu CSQOUTIL , který je zdokumentován v tématu [Obslužný program zásad zabezpečení zpráv \(CSQOUTIL\)](#).

Použijte obslužný program CSQOUTIL ke spuštění následujícího příkazu pro definování zásady integrity pro vzdálenou frontu na BNK6:

```
setmqsp1 -m BNK6 -p FIN.XFER.Q7 -s MD5 -a CN=Teller5,O=BCO,C=US
```

V této zásadě je správce front identifikován jako BNK6. Název zásady a přidružená fronta je FIN.XFER.Q7. Algoritmus použitý ke generování podpisu odesílatele je MD5a rozlišující název (DN) odesílajícího uživatele je 'CN=Teller5,O=BCO,C=US'.

Použijte také obslužný program CSQOUTIL a spusťte následující příkaz k definování zásady integrity pro lokální frontu na BNK7:

```
setmqsp1 -m BNK7 -p FIN.RCPT.Q7 -s MD5 -a CN=Teller5,O=BCO,C=US
```

V této zásadě je správce front identifikován jako BNK7. Název zásady a přidružená fronta je FIN.RCPT.Q7. Algoritmus očekávaný pro podpis odesílatele je MD5a očekává se, že rozlišující název (DN) odesílajícího uživatele bude 'CN=Teller5,O=BCO,C=US'.

Po definování těchto dvou zásad restartujte správce front BNK6 a BNK7 nebo pomocí příkazu z/OS **MODIFY** aktualizujte konfigurace zásad produktu IBM MQ Advanced Message Security . Příklad:

Dne BNK6:

```
F BNK6AMSM, REFRESH, POLICY
```

V BNK7:

```
F BNK7AMSM, REFRESH, POLICY
```

## Vzdálené ukládání zpráv chráněných ochranou soukromí do fronty v systému z/OS

Tento příklad podrobně popisuje zásady a certifikáty produktu IBM MQ Advanced Message Security potřebné k odesílání a načítání zpráv chráněných soukromě a z front spravovaných dvěma různými správci front. Dva správci front mohou být spuštěni ve stejném systému z/OS nebo v různých systémech z/OS, nebo jeden správce front může být na distribuovaném systému, na kterém běží IBM MQ Advanced Message Security.

Příklad správců front a front jsou:

```
BNK6          - Sending queue manager
BNK7          - Recipient queue manager
FIN.XFER.Q7   - Remote queue on BNK6
FIN.RCPT.Q7   - Local queue on BNK7
```

Poznámka: V tomto příkladu jsou správci front BNK6 a BNK7 správci front spuštěni na různých systémech z/OS se stejným názvem.

Tito uživatelé se používají:

```
WMQBNK6      - IBM MQ AMS task user on BNK6
WMQBNK7      - IBM MQ AMS task user on BNK7
TELLER5      - Sending user on BNK6
FINADM2      - Recipient user on BNK7
```

Postup konfigurace tohoto scénáře je následující:

### Vytvoření uživatelských certifikátů

V tomto příkladu se požadují dva uživatelské certifikáty. Jedná se o odesílaný uživatelský certifikát, který je nutný pro podepisování zpráv, a certifikát uživatele příjemce, který je potřebný pro šifrování a dešifrování dat zprávy. Odesílající uživatel je 'TELLER5' a uživatel příjemce je 'FINADM2'.

Je také požadován certifikát vydavatele certifikátů (CA). Certifikát CA je certifikát autority, která vydala certifikát uživatele. Může se jednat o řetězec certifikátů. Je-li tomu tak, všechny certifikáty v řetězci jsou vyžadovány v svazku klíčů uživatele úlohy IBM MQ Advanced Message Security, v tomto případě uživatele WMQBNK7.

Certifikát CA lze vytvořit pomocí příkazu RACDCERT produktu RACF. Tento certifikát se používá k vydávání uživatelských certifikátů. Příklad:

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('BCOCA') O('BCO') C('US'))
KEYUSAGE(CERTSIGN) WITHLABEL('BCOCA')
```

Tento příkaz RACDCERT vytvoří certifikát CA, který pak může být použit k vydávání uživatelských certifikátů pro uživatele 'TELLER5' a 'FINADM2'. Příklad:

```
RACDCERT ID(TELLER5) GENCERT SUBJECTSDN(CN('Teller5') O('BCO') C('US'))
WITHLABEL('Teller5') SIGNWITH(CERTAUTH LABEL('BCOCA'))
KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)

RACDCERT ID(FINADM2) GENCERT SUBJECTSDN(CN('FinAdm2') O('BCO') C('US'))
WITHLABEL('FinAdm2') SIGNWITH(CERTAUTH LABEL('BCOCA'))
KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)
```

Vaše instalace bude mít procedury pro výběr nebo vytvoření certifikátu CA, stejně jako procedury pro vydávání certifikátů a distribuci těchto certifikátů do příslušných systémů.

Při exportu a importu těchto certifikátů produkt IBM MQ Advanced Message Security vyžaduje:

- Certifikát CA (řetězec).
- Odesílající uživatelský certifikát a jeho soukromý klíč.
- Certifikát uživatele příjemce a jeho soukromý klíč.

Používáte-li produkt RACF, lze příkaz RACDCERT EXPORT použít k exportování certifikátů do datové sady a příkaz RACDCERT ADD lze použít k importování certifikátů z datové sady. Další informace o těchto a dalších příkazech RACDCERT naleznete v příručce *z/OS: Security Server RACF Command Language Reference*.

Certifikáty v tomto případě jsou vyžadovány na systému z/OS se spuštěným správcem front BNK6 a BNK7.

V tomto příkladu musí být odesílající a přijímající certifikáty importovány na systém z/OS s operačním systémem BNK6 a certifikáty CA a příjemce musí být importovány do systému z/OS, kde je spuštěna BNK7. Když certifikáty byly importovány, uživatelské certifikáty vyžadují atribut TRUST. Příkaz RACDCERT ALTER lze použít k přidání atributu TRUST do certifikátu. Příklad:

Dne BNK6:

```
RACDCERT ID(TELLER5) ALTER (LABEL('Teller5')) TRUST
RACDCERT ID(FINADM2) ALTER (LABEL('FinAdm2')) TRUST
```

V BNK7:

```
RACDCERT ID(FINADM2) ALTER (LABEL('FinAdm2')) TRUST
```

## Připojení certifikátů k příslušným klíčovým sdružením

Pokud byly požadované certifikáty vytvořeny nebo importovány a nastaveny jako důvěryhodné, musí být připojeny k příslušným klíčům uživatelských klíčů na systémech z/OS s operačním systémem BNK6 a BNK7.

Chcete-li vytvořit svazky klíčů, použijte příkaz RACDCERT ADDRING:

Dne BNK6:

```
RACDCERT ID(WMQBNK6) ADDRING(drq.ams.keyring)
RACDCERT ID(TELLER5) ADDRING(drq.ams.keyring)
```

Tím se vytvoří svazek klíčů pro uživatele úlohy IBM MQ Advanced Message Security a svazek klíčů pro odeslání uživatele na BNK6. Mějte na zřeteli, že název svazku klíčů drq.ams.keyring je povinný a název rozlišuje velká a malá písmena.

V BNK7:

```
RACDCERT ID(WMQBNK7) ADDRING(drq.ams.keyring)
RACDCERT ID(FINADM2) ADDRING(drq.ams.keyring)
```

Tím se vytvoří svazek klíčů pro uživatele úlohy IBM MQ Advanced Message Security a svazek klíčů pro uživatele příjemce na BNK7.

Když byly vytvořeny svazky klíčů, mohou být příslušné certifikáty připojeny.

Dne BNK6:

```
RACDCERT ID(WMQBNK6) CONNECT(ID(FINADM2) LABEL('FinAdm2')
RING(drq.ams.keyring) USAGE(SITE))
```

```
RACDCERT ID(TELLER5) CONNECT(ID(TELLER5) LABEL('Teller5'))  
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
```

V BNK7:

```
RACDCERT ID(WMQBNK7) CONNECT(CERTAUTH LABEL('BCOCA'))  
RING(drq.ams.keyring)
```

```
RACDCERT ID(FINADM2) CONNECT(ID(FINADM2) LABEL('FinAdm2'))  
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
```

Odesílající a přijímající uživatelské certifikáty musí být připojeny jako DEFAULT. Má-li uživatel více než jeden certifikát ve svém souboru drq.ams.keyring, použijte se výchozí certifikát pro podepisování a pro účely šifrování/dešifrování.

V případě BNK6 musí být certifikát uživatele příjemce také připojen ke klíčovému okruhu uživatele úlohy IBM MQ Advanced Message Security s USAGE (SITE). Důvodem je to, že úloha zabezpečení rozšířených zpráv potřebuje veřejný klíč příjemce při šifrování dat zprávy. USAGE (SITE) zabraňuje tomu, aby byl soukromý klíč přístupný v klíčovém kruhu.

Vytvoření a úprava certifikátů nejsou produktem IBM MQ Advanced Message Security rozpoznány, dokud není správce front zastaven a restartován, nebo se příkaz z/OS **MODIFY** používá k aktualizaci konfigurace certifikátu produktu IBM MQ Advanced Message Security . Příklad:

Dne BNK6:

```
F BNK6AMSM, REFRESH, KEYRING
```

V BNK7:

```
F BNK7AMSM, REFRESH, KEYRING
```

## Vytvoření zásad produktu IBM MQ Advanced Message Security

V tomto příkladu jsou zprávy chráněné soukromě vloženy do vzdálené fronty FIN.XFER.Q7 na BNK6 aplikací spuštěnou jako uživatel 'TELLER5' a načtené z lokální fronty FIN.RCPT.Q7 na BNK7 aplikací spuštěnou jako uživatel 'FINADM2', takže jsou vyžadovány dvě zásady IBM MQ Advanced Message Security .

Zásady produktu IBM MQ Advanced Message Security se vytvářejí pomocí obslužného programu CSQOUTIL , který je zdokumentován v tématu [Obslužný program zásad zabezpečení zpráv \(CSQOUTIL\)](#).

Použijte obslužný program CSQOUTIL pro spuštění následujícího příkazu k definování zásady ochrany osobních údajů pro vzdálenou frontu na BNK6:

```
setmqsp1 -m BNK6 -p FIN.XFER.Q7 -s SHA1 -e 3DES -a CN=Teller5,O=BCO,C=US -r  
CN=FinAdm2,O=BCO,C=US
```

V této zásadě je správce front identifikován jako BNK6. Název zásady a přidružená fronta je FIN.XFER.Q7. Algoritmus použitý ke generování podpisu odesílatele je SHA1, rozlišující název (DN) odesílajícího uživatele je 'CN=Teller5,O=BCO,C=US' a uživatel příjemce je 'CN=FinAdm2,O=BCO,C=US'. Algoritmus, který se používá k šifrování dat zprávy, je 3DES.

Použijte také obslužný program CSQOUTIL a spusťte následující příkaz k definování zásady ochrany osobních údajů pro lokální frontu na BNK7:

```
setmqsp1 -m BNK7 -p FIN.RCPT.Q7 -s SHA1 -e 3DES -a CN=Teller5,O=BCO,C=US -r  
CN=FinAdm2,O=BCO,C=US
```

V této zásadě je správce front identifikován jako BNK7. Název zásady a přidružená fronta je FIN.RCPT.Q7. Algoritmus očekávaný pro podpis odesílatele je SHA1, očekává se, že rozlišující název (DN) odesílajícího uživatele bude 'CN=Teller5,O=BCO,C=US', a uživatel příjemce je 'CN=FinAdm2,O=BCO,C=US'. Algoritmus, který se používá k dešifrování dat zprávy, je 3DES.

Po definování těchto dvou zásad restartujte správce front BNK6 a BNK7 , nebo pomocí příkazu z/OS **MODIFY** obnovte konfiguraci zásady produktu IBM MQ Advanced Message Security . Příklad:

Dne BNK6:

```
F BNK6AMSM,REFRESH,POLICY
```

V BNK7:

```
F BNK7AMSM,REFRESH,POLICY
```

## 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 popsanych 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 popsany 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 směřovány 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 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.com jsou 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](http://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: